INSTITUTO DE MATEMÁTICA PURA E APLICADA

Introdução à

Teoria dos Números

José Plínio de Oliveira Santos

Impresso no Brasil/Printed in Brazil

Capa: Noni Geiger e Rodolfo Capeto

Coleção Matemática Universitária

Títulos publicados:

1. *Análise Real, Volume 1* (Terceira Edição) – Elon Lages Lima
2. *EDP: Um Curso Introdutório* - Valéria Iório
3. *Curso de Álgebra, Volume 1* (Segunda Edição) – Abramo Hefez
4. *Introdução às Curvas Algébricas Planas* – Israel Vainsencher
5. *Álgebra Linear* (Terceira Edição) – Elon Lages Lima
6. *Equações Diferenciais Aplicadas* – Djairo G. de Figueiredo e Aloisio Freiria Neves
7. *Geometria Diferencial* – Paulo Ventura Araújo
8. *Introdução à Teoria dos Números* – José Plínio de Oliveira Santos

Diagramação:
CRAFTEX Comunicação Visual, Tel. 512.9944
Rio de Janeiro, RJ
e-mail: home@craftex.com.br
web: http://www.craftex.com.br

Distribuição:
SBM, Sociedade Brasileira de Matemática
Estrada Dona Castorina, 110
22460-320, Rio de Janeiro, RJ
e-mail: sbm@impa.br
Web: http://www.sbm.org

Prefácio

Este livro surgiu a partir de notas de aula utilizadas nos últimos 4 anos num curso introdutório de Teoria dos Números que ministramos na Unicamp.

O estudo das propriedades dos números inteiros positivos é o objetivo central da Teoria dos Números. São três os principais ramos em que se divide a Teoria dos Números: Teoria Elementar, Teoria Analítica e Teoria Algébrica. Neste livro nos limitamos à parte elementar, onde apresentamos resultados básicos, não apenas para o estudo das partes Analítica e Algébrica, como também, para os demais ramos da matemática.

Introduzimos os conceitos através de um significativo número de exemplos procurando, desta forma, motivar o leitor antes deste ter contato com demonstrações formais. Vale mencionar aqui que, em Teoria dos Números, esta tarefa não é difícil, pois é grande o número de problemas interessantes que não requerem ferramentas sofisticadas para a sua compreensão.

Fornecemos, a seguir, uma breve descrição de cada capítulo.

No Capítulo 1, estudamos propriedades elementares sobre divisibilidade no conjunto dos inteiros, sendo o Algoritmo da Divisão (Teorema 1.2) o resultado mais importante. Duas das várias provas da infinitude dos primos são fornecidas.

No Capítulo 2, introduzimos o importantíssimo conceito de congruência onde a contribuição de Gauss foi fundamental. Teoremas de Euler, Fermat e Wilson são apresentados, não deixando de discutir o chamado Teorema do Resto Chinês.

O Princípio da Casa dos Pombos, apresentado no Capítulo 3, nem sempre é encontrado em textos introdutórios como este. Nosso objetivo, ao fazer isto, foi o de apresentar alguns aspectos combinatórios relacionados com Teoria dos Números. Demonstrações combinatórias para o Pequeno Teorema de Fermat e para o Teorema de Wilson são apresentadas neste Capítulo.

No Capítulo 4, introduzimos algumas importantes funções aritméticas e relações entre elas. Além de uma caracterização dos números perfeitos pares dada por Euclides e Euler, introduzimos a importantíssima sequência dos

Números de Fibonacci.

No estudo de Resíduos Quadráticos, feito no Capítulo 5, introduzimos o Símbolo de Legendre que nos permite obter informações sobre a existência ou não de soluções para a congruência $x^2 \equiv a(\bmod p)$. Nisto também contribuiram, de forma fundamental, Euler e Gauss. Apresentamos uma das várias demonstrações existentes da chamada Lei de Reciprocidade Quadrática de Gauss.

Uma completa caracterização dos números que possuem raízes primitivas é dada no Capítulo 6.

No Capítulo 7, fornecemos alguns resultados clássicos sobre a representação de inteiros como soma de quadrados.

Frações contínuas, objeto de estudo no Capítulo 8, é uma vasta área em Teoria dos Números, da qual apresentamos apenas alguns importantes resultados dentre os quais destacamos a obtenção de aproximações de irracionais por racionais.

O conceito de Partições de um inteiro, onde Euler contribuiu de maneira fundamental, é introduzido no Capítulo 9. Fornecemos, neste capítulo, uma demonstração combinatória para o Teorema dos Números Pentagonais de Euler.

A equivalência entre as Primeira e Segunda formas do Princípio da Indução Finita e o Princípio da Boa Ordem é dada no Apêndice A. No Apêndice B, apresentamos mais duas provas da infinitude dos primos. Um interessante resultado sobre a distribuição dos primos, O Postulado de Bertrand, é fornecido no Apêndice C.

Ao colega Paulo Mondek, pelos erros apontados e valiosas sugestões dadas, meus sinceros agradecimentos. Agradeço, também, aos vários alunos que utilizaram estas notas nos últimos semestres destacando, pelas inúmeras sugestões, Augusto Cesar Ponce e Eduardo Bovo.

Finalmente, pelo excelente trabalho de digitação, agradeço a Flávio Rodrigues de Andrade.

Campinas, 20 de agosto de 1998.
José Plínio de Oliveira Santos

Sumário

Capítulo 1

Divisibilidade

Neste capítulo são apresentados vários resultados básicos de extrema importância. O Teorema 1.2, sobre a existência e unicidade do quociente e do resto na divisão de inteiros, e o Teorema Fundamental da Aritmética (Teorema 1.9), sobre a unicidade da representação de um inteiro como produto de potências de primos, são os mais importantes.

Uma das várias provas da existência de infinitos primos é apresentada no Teorema 1.12.

1.1 Indução

Iniciamos este capítulo com a discussão de uma indispensável ferramenta na demonstração de muitos teoremas: o Princípio da Indução Finita. Enunciamos, abaixo, duas formas deste princípio e, também, o Princípio da Boa Ordem.

A_0. Princípio da Boa Ordem (PBO)

Todo conjunto não-vazio de inteiros positivos contém um elemento mínimo.

A_1. Primeira forma do Princípio de Indução Finita

Seja B um subconjunto dos inteiros positivos. Se B possui as duas seguintes propriedades

(i) $1 \in B$
(ii) $k + 1 \in B$ sempre que $k \in B$

então B contém todos os inteiros positivos.

A_2. Segunda forma do Princípio de Indução Finita

Seja B um subconjunto dos inteiros positivos. Se B possui as duas seguintes propriedades
(i) $1 \in B$
(ii) $k+1 \in B$ sempre que $1, 2, \ldots, k \in B$
então B contém todos os inteiros positivos.

Com a finalidade de demonstrarmos o Princípio de Indução Finita nós assumimos o Princípio da Boa Ordem como um postulado. Na realidade, como A_0, A_1 e A_2 são equivalentes (veja Apêndice A para uma demonstração), poderíamos ter assumido, indiferentemente A_1 ou A_2 como tal. Vamos, pois, demonstrar A_1 tendo como hipótese o Princípio da Boa Ordem.

Desejamos provar que se B é um subconjunto dos inteiros positivos, possuindo as propriedades (i) e (ii), então B, necessariamente, contém todos os inteiros positivos. A prova que apresentamos é por contradição. Vamos supor que, mesmo possuindo as propriedades (i) e (ii) B não contenha todos os inteiros positivos. Seja A o conjunto dos inteiros positivos não contidos em B. Pelo PBO, A possui um menor elemento e este é maior do que 1 pois $1 \in B$. Seja a_0 este elemento. É claro que $a_0 - 1$ pertence a B e como B satisfaz (ii) então o sucessor de $a_0 - 1$, que é a_0, também deve pertencer a B. Esta contradição nos leva a concluir que A tem que ser vazio, o que conclui a demonstração. □

Exemplo 1.1 Mostre que

$$1 + x + x^2 + \cdots + x^{n-1} = \frac{x^n - 1}{x - 1}.$$

Devemos mostrar que para $n = 1$ a expressão acima é verdadeira, isto é,

$$x^0 = 1 = \frac{x-1}{x-1}.$$

Assumimos, agora, a validade da mesma para $n-1$ e utilizando isto mostramos que a expressão também se verifica para n. Logo temos:

$$\begin{aligned}\sum_{i=0}^{n} x^i &= \sum_{i=0}^{n-1} x^i + x^n \\ &= (1 + x + x^2 + \cdots + x^{n-1}) + x^n \\ &= \frac{x^n - 1}{x - 1} + x^n = \frac{x^n - 1 + (x-1)x^n}{x-1} = \frac{x^{n+1} - 1}{x - 1}.\end{aligned}$$

Desta forma a condição (ii) está verificada e, pelo Princípio de Indução Finita, podemos concluir a validade desta fórmula para todo inteiro positivo.

1.2 Divisibilidade

Definição 1.1 Se a e b são inteiros, dizemos que a *divide* b, denotando por $a|b$, se existir um inteiro c tal que $b = ac$.
Se a não divide b escrevemos $a \nmid b$.

Proposição 1.1 *Se* a, b *e* c *são inteiros,* $a|b$ *e* $b|c$, *então* $a|c$.

Demonstração: Como $a|b$ e $b|c$, existem inteiros k_1 e k_2 com $b = k_1 a$ e $c = k_2 b$. Substituindo o valor de b na equação $c = k_2 b$ teremos $c = k_2 k_1 a$ o que implica $a|c$. □

Exemplo 1.2 Como $3|12$ e $12|48$, então $3|48$. Como não existe inteiro c satisfazendo $15 = 4 \cdot c$, então $4 \nmid 15$.

Proposição 1.2 *Se* a, b, c, m *e* n *são inteiros,* $c|a$ *e* $c|b$ *então* $c|(ma + nb)$.

Demonstração: Se $c|a$ e $c|b$ então $a = k_1 c$ e $b = k_2 c$. Multiplicando-se estas duas equações respectivamente por m e n teremos $ma = mk_1 c$ e $nb = nk_2 c$. Somando-se membro a membro obtemos $ma + nb = (mk_1 + nk_2)c$, o que nos diz que $c|(ma + nb)$. □

Exemplo 1.3: Como $3|15$ e $3|42$, então $3|(8 \times 15 - 7 \times 42)$.

Teorema 1.1 *A divisão tem as seguintes propriedades:*

(i) $n|n$

(ii) $d|n \Rightarrow ad|an$

(iii) $ad|an$ e $a \neq 0 \Rightarrow d|n$

(iv) $1|n$

(v) $n|0$

(vi) $d|n$ e $n \neq 0 \Rightarrow |d| \leq |n|$

(vii) $d|n$ e $n|d \Rightarrow |d| = |n|$

(viii) $d|n$ e $d \neq 0 \Rightarrow (n/d)|n$.

Demonstração: (i) Como $n = 1 \cdot n$ segue da definição que $n|n$, inclusive para $n = 0$. (ii) Se $d|n$ então $n = cd$ para algum inteiro c. Logo $an = cad$ o que conclui a demonstração.

Demonstramos, agora, (viii). Se $d|n$ então $n = k_1 d$ e portanto n/d é um inteiro. Como $(n/d) \cdot d = n$ segue da definição que $(n/d)|n$. Os demais

itens também são conseqüência imediata da definição e serão deixados como exercício. □

Antes de introduzirmos o algoritmo da divisão (ele aparece no livro VII dos "Elementos" de Euclides, escrito por volta do ano 300 a.C.), enunciamos o chamado Teorema de Eudoxius*: Dados a e b inteiros com $b \neq 0$ então a é um múltiplo de b ou se encontra entre dois múltiplos consecutivos de b, isto é, correspondendo a cada par de inteiros a e $b \neq 0$ existe um inteiro q tal que, para $b > 0$,

$$qb \leq a < (q+1)b \tag{1.1}$$

e para $b < 0$,

$$qb \leq a < (q-1)b. \tag{1.2}$$

Exemplo 1.4 Se $a = 11$ e $b = 4$, devemos tomar $q = 2$

$$2 \times 4 \leq 11 < 3 \times 4 \, .$$

Para $a = -11$ e $b = 4$, tomamos $q = -3$

$$-3 \times 4 \leq -11 < (-3+1) \times 4 \, .$$

Se $a = 11$ e $b = -4$, tomamos $q = -2$

$$(-2) \times (-4) \leq 11 < (-2-1) \times (-4) \, .$$

Para $a = -11$ e $b = -4$, tomamos $q = 3$

$$3 \times (-4) \leq -11 < (3-1) \times (-4).$$

1.3 O Algoritmo da Divisão

Teorema 1.2 *Dados dois inteiros* a *e* $b, b > 0$, *existe um único par de inteiros* q *e* r *tais que*

$$a = qb + r, \quad \text{com} \quad 0 \leq r < b \qquad (r = 0 \Leftrightarrow b|a)$$

(q é chamado de *quociente* e r de *resto* da divisão de a por b).

*Este resultado costuma ser erroneamente atribuído a Arquimedes e chamado "Princípio de Arquimedes".

Demonstração: Pelo Teorema de Eudoxius, como $b > 0$, existe q satisfazendo:

$$qb \leq a < (q+1)b$$

o que implica $0 \leq a - qb$ e $a - qb < b$. Desta forma, se definirmos $r = a - qb$, teremos, garantida, a existência de q e r. A fim de mostrarmos a unicidade, vamos supor a existência de outro par q_1 e r_1 verificando:

$$a = q_1 b + r_1 \qquad \text{com} \qquad 0 \leq r_1 < b.$$

Disto temos $(qb + r) - (q_1 b + r_1) = 0 \Rightarrow b(q - q_1) = r_1 - r$, o que implica $b|(r_1 - r)$. Mas, como $r_1 < b$ e $r < b$, temos $|r_1 - r| < b$ e, portanto, como $b|(r_1 - r)$ devemos ter $r_1 - r = 0$ o que implica $r = r_1$. Logo $q_1 b = qb \Rightarrow q_1 = q$, uma vez que $b \neq 0$. □

Observação: Embora no enunciado do Teorema 1.2 exista a restrição $b > 0$, isto não é necessário e, utilizando-se a equação (1.2) teríamos encontrado q e r também para $b < 0$. Podemos, pois, enunciar o Algoritmo da Divisão de Euclides da seguinte forma: Dados dois inteiros a e $b, b \neq 0$ existe um único par de inteiros q e r tais que $a = qb + r$ com $0 \leq r < |b|$.

1.4 O Máximo Divisor Comum

O *máximo divisor comum* de dois inteiros a e b (a ou b diferente de zero), denotado por (a, b), é o maior inteiro que divide a e b.

Teorema 1.3 Seja d o máximo divisor comum de a e b, então existem inteiros n_0 e m_0 tais que $d = n_0 a + m_0 b$.

Demonstração: Seja B o conjunto de todas as combinações lineares $\{na + mb\}$ onde n e m são inteiros. Este conjunto contém, claramente, números negativos, positivos e também o zero. Vamos escolher n_0 e m_0 tais que $c = n_0 a + m_0 b$ seja o menor inteiro positivo pertencente ao conjunto B. Vamos provar que $c|a$ e $c|b$. Como as demonstrações são similares, mostraremos apenas que $c|a$. A prova é por contradição. Suponhamos que $c \nmid a$. Neste caso, pelo Teorema 1.2, existem q e r tais que $a = qc + r$ com $0 < r < c$. Portanto $r = a - qc = a - q(n_0 a + m_0 b) = (1 - qn_0)a + (-qm_0)b$. Isto mostra que $r \in B$, pois $(1 - qn_0)$ e $(-qm_0)$ são inteiros, o que é uma contradição, uma vez que $0 < r < c$ e c é o menor elemento positivo de B. Logo $c|a$ e de forma análoga se prova que $c|b$.

Como d é um divisor comum de a e b, existem inteiros k_1 e k_2 tais que $a = k_1 d$ e $b = k_2 d$ e, portanto, $c = n_0 a + m_0 b = n_0 k_1 d + m_0 k_2 d = d(n_0 k_1 + m_0 k_2)$ o que implica $d|c$. Do Teorema 1.1 (vi), temos que $d \leq c$ (ambos são positivos)

e como $d < c$ não é possível, uma vez que d é o máximo divisor comum, concluímos que $d = n_0a + m_0b$. □

Observação: Na demonstração deste teorema mostramos, não apenas que o máximo divisor comum de a e b pode ser expresso como uma combinação linear destes números mas que este número é o menor valor positivo dentre todas estas combinações lineares. O teorema seguinte nos dá uma outra caracterização para o máximo divisor comum de dois números.

Teorema 1.4 *O máximo divisor comum* d *de* a *e* b *é o divisor positivo de* a *e* b *o qual é divisível por todo divisor comum.*

Demonstração: Do teorema anterior e pela Proposição 1.2 concluímos que se d_1 é divisor comum de a e b, então $d_1|d$. Portanto não podem existir dois números tendo cada um a propriedade de ser divisível por todo divisor comum. Isto por causa do Teorema 1.1 (vii) que, no caso de números positivos d_1 e d, nos diz que d_1 deve ser igual a d. □

Proposição 1.3. *Para todo inteiro positivo* t, $(ta, tb) = t(a, b)$.

Demonstração: Pelo Teorema 1.3 (ta, tb) é o menor valor positivo de $mta + ntb$ (m e n inteiros), que é igual a t vezes o menor valor positivo de $ma+nb = t \cdot (a, b)$. □

Proposição 1.4 *Se* $c > 0$ *e* a *e* b *são divisíveis por* c, *então*

$$\left(\frac{a}{c}, \frac{b}{c}\right) = \frac{1}{c}(a, b).$$

Demonstração: Como a e b são divisíveis por c, temos que a/c e b/c são inteiros. Basta, então, substituir na Proposição 1.3 "a"por "a/c"e "b"por "b/c"tomando $t = c$. □

Corolário: *Se* $(a, b) = d$, *temos que* $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

Demonstração: No que acabamos de demonstrar c é um divisor comum de a e b. Se tomarmos c como sendo o máximo divisor comum d, teremos o resultado desejado. □

Exemplo 1.5 Como (14,35) = 7 temos que (14/7, 35/7) = 1.

Definição 1.2. Os inteiros a e b são relativamente primos quando $(a, b) = 1$.

Teorema 1.5. *Para* a, b *e* x *inteiros temos* $(a, b) = (a, b + ax)$.

Demonstração: Sejam $d = (a, b)$ e $f = (a, b + ax)$. Pelo Teorema 1.3 existem inteiros n_0 e m_0 tais que $d = n_0a + m_0b$ e como esta expressão pode ser escrita

como $d = a(n_0 - xm_0) + (b + ax)m_0$, concluímos que o máximo divisor f de a e $b + ax$ é um divisor de d. Tendo mostrado que $f|d$ mostramos, a seguir, que $d|f$. Pela Proposição 1.2, $d|(b + ax)$ e pelo Teorema 1.4 sabemos que todo divisor comum de a e $b + ax$ é um divisor de f. Tendo, assim, provado que $d|f$ concluímos, pelo Teorema 1.1 (vii), que $d = f$, uma vez que ambos são positivos. □

Exemplo 1.6: (3, 15)=(3, 15+4 × 3)=(3, 15+7 × 3) =(3, 15−8 × 3)...

Teorema 1.6. *Se* $a|bc$ *e* $(a, b) = 1$, *então* $a|c$.

Demonstração: Como $(a, b) = 1$ pelo Teorema 1.3 existem inteiros n e m tais que $na + mb = 1$. Multiplicando-se os dois lados desta igualdade por c temos: $n(ac) + m(bc) = c$. Como $a|ac$ e, por hipótese, $a|bc$ então, pela Proposição 1.2, $a|c$. □

Exemplo: $4|(27 \times 20)$, logo $4|20$ uma vez que $(4, 27) = 1$.

O teorema seguinte nos apresenta um resultado elementar, mas de grande importância na demonstração do Algoritmo de Euclides (Teorema 1.8).

Teorema 1.7. *Se* a *e* b *são inteiros e* $a = qb + r$ *onde* q *e* r *são inteiros, então* $(a, b) = (b, r)$.

Demonstração: Da relação $a = qb + r$ podemos concluir que todo divisor de b e r é um divisor de a (Proposição 1.2). Esta mesma relação, escrita na forma $r = a - qb$, nos diz que todo divisor de a e b é um divisor de r. Logo o conjunto dos divisores comuns de a e b é igual ao conjunto dos divisores comuns de b e r, o que nos garante o resultado $(a, b) = (b, r)$. □

Vamos descrever, através de um exemplo, a idéia utilizada na demonstração do Teorema 1.8. Estamos interessados no cálculo do máximo divisor comum de 1126 e 522. Utilizamos o Algoritmo da Divisão (Teorema 1.2) para dividir 1126 por 522. Em seguida dividimos 522 pelo resto 82. Depois 82 pelo resto 30 e assim, sucessivamente, até obtermos resto zero.

$$\begin{aligned}
1126 &= 2 \times 522 + 82 \\
522 &= 6 \times 82 + 30 \\
82 &= 2 \times 30 + 22 \\
30 &= 1 \times 22 + 8 \\
22 &= 2 \times 8 + 6 \\
8 &= 1 \times 6 + 2 \\
6 &= 3 \times 2 + 0
\end{aligned}$$

Da última equação temos que $(6, 2) = 2$ e agora, pelo Teorema 1.7, podemos concluir da equação 8=1 × 6+2, que (8,6) = (6,2), da equação 22=2 ×

8+6 que (22,8) = (8,6) e, por sucessivas aplicações do Teorema 1.7, construir a seqüência de igualdades $(2,6) = (6,8) = (8,22) = (22,30) = (30,82) = (82,522) = (522,1126)$. Tendo encontrado, desta forma, o máximo divisor comum de 522 e 1126 que é o último resto não-nulo da seqüência de igualdades acima.

1.5 O Algoritmo de Euclides

Teorema 1.8. *Sejam* $r_0 = a$ *e* $r_1 = b$ *inteiros não-negativos com* $b \neq 0$. *Se o algoritmo da divisão for aplicado sucessivamente para se obter*

$$r_j = q_{j+1}r_{j+1} + r_{j+2}, \; 0 \leq r_{j+2} < r_{j+1}$$

para $j = 0, 1, 2, \ldots, n-1$ *e* $r_{n+1} = 0$ *então* $(a, b) = r_n$, *o último resto não-nulo.*

Demonstração: Tendo em mente o exemplo anterior fica fácil acompanhar a demonstração deste algoritmo. Vamos, inicialmente, aplicar o Teorema 1.2 para dividir $r_0 = a$ por $r_1 = b$ obtendo $r_0 = q_1r_1 + r_2$, em seguida dividimos r_1 por r_2 obtendo $r_1 = q_2r_2 + r_3$ e assim, sucessivamente, até a obtenção do resto $r_{n+1} = 0$. Como, a cada passo o resto é sempre menor do que o anterior, e estamos lidando com números inteiros positivos, é claro que após um número finito de aplicações do Teorema 1.2, teremos resto nulo.

Temos, pois, a seguinte seqüência de equações:

$$\begin{array}{ll} r_0 = q_1r_1 + r_2 & 0 < r_2 < r_1 \\ r_1 = q_2r_2 + r_3 & 0 < r_3 < r_2 \\ r_2 = q_3r_3 + r_4 & 0 < r_4 < r_3 \\ \vdots & \\ r_{n-2} = q_{n-1}r_{n-1} + r_n & 0 < r_n < r_{n-1} \\ r_{n-1} = q_nr_n + 0. & \end{array}$$

A última destas equações nos diz, pelo Teorema 1.7, que o máximo divisor comum de r_n e r_{n-1} é r_n. A penúltima, que este número é igual a (r_{n-1}, r_{n-2}) e, prosseguindo desta maneira teremos, por repetidas aplicações do Teorema 1.7, a seqüência:

$$r_n = (r_{n-1}, r_n) = (r_{n-2}, r_{n-1}) = \cdots\cdots = (r_1, r_2) = (r_0, r_1) = (a, b).$$

Portanto o máximo divisor comum de a e b é o último resto não-nulo da seqüência de divisões descrita. □

1.6 Números Primos

Definição 1.3 Um número inteiro $n (n > 1)$ possuindo somente dois divisores positivos n e 1 é chamado *primo*.

Se $n > 1$ não é primo dizemos que n é *composto*.

Proposição 1.4. *Se* $p|ab$, p *primo, então* $p|a$ *ou* $p|b$.

Demonstração: Se $p \nmid a$, então $(a, p) = 1$ o que implica, pelo Teorema 1.6, $p|b$. □

Teorema 1.9. (Teorema Fundamental da Aritmética) *Todo inteiro maior do que 1 pode ser representado de maneira única (a menos da ordem) como um produto de fatores primos.*

Demonstração: Se n é primo não há nada a ser demonstrado. Suponhamos, pois, n composto. Seja $p_1 (p_1 > 1)$ o menor dos divisores positivos de n. Afirmamos que p_1 é primo. Isto é verdade, pois, caso contrário existiria p, $1 < p < p_1$ com $p|n$, contradizendo a escolha de p_1. Logo, $n = p_1n_1$.

Se n_1 for primo a prova está completa. Caso contrário, tomamos p_2 como o menor fator de n_1. Pelo argumento anterior, p_2 é primo e temos que $n = p_1p_2n_2$.

Repetindo este procedimento, obtemos uma seqüência decrescente de inteiros positivos $n_1, n_2, \ldots, n_r$. Como todos eles são inteiros maiores do que 1, este processo deve terminar. Como os primos na seqüência $p_1, p_2, \ldots, p_k$ não são, necessariamente, distintos, n terá, em geral, a forma:

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}.$$

Para mostrarmos a unicidade usamos indução em n. Para $n = 2$ a afirmação é verdadeira. Assumimos, então, que ela se verifica para todos os inteiros maiores do que 1 e menores do que n. Vamos provar que ela também é verdadeira para n. Se n é primo, não há nada a provar. Vamos supor, então, que n seja composto e que tenha duas fatorações, isto é,

$$n = p_1p_2 \cdots p_s = q_1q_2 \cdots q_r.$$

Vamos provar que $s = r$ e que cada p_i é igual a algum q_j. Como p_1 divide o produto $q_1q_2 \cdots q_r$ ele divide pelo menos um dos fatores q_j. Sem perda de generalidade podemos supor que $p_1|q_1$. Como são ambos primos, isto implica $p_1 = q_1$. Logo $n/p_1 = p_2 \cdots p_s = q_2 \cdots q_r$. Como $1 < n/p_1 < n$, a hipótese de indução nos diz que as duas fatorações são idênticas, isto é, $s = r$ e, a menos da ordem, as fatorações $p_1p_2 \cdots p_s$ e $q_1q_2 \cdots q_s$ são iguais. □

Teorema 1.10. *Se* $n = \prod_{i=1}^{r} p_i^{a_i}$, *o conjunto dos divisores positivos de* n *é o conjunto de todos os números da forma*

$$\prod_{i=1}^{r} p_i^{c_i}, \quad 0 \le c_i \le a_i, \quad i = 1, 2, \ldots r.$$

Demonstração: É óbvio que se c_i não estiver no intervalo mencionado, o produto acima não será um divisor de n. □

Mencionamos isto como um teorema para dar destaque a este resultado, embora elementar.

Observação: Se denotarmos a seqüência de primos em ordem crescente $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7, \ldots, p_n$=enésimo primo, então todo inteiro positivo pode ser escrito na forma

$$n = \prod_{i=1}^{\infty} p_i^{a_i}, \ a_i \ge 0.$$

Os divisores positivos de n são, agora, todos os números da forma

$$\prod_{i=1}^{\infty} p_i^{c_i}, \ 0 \le c_i \le a_i.$$

Todos estes produtos são finitos pois o número de fatores primos de qualquer inteiro é sempre finito.

Teorema 1.11 *Se dois inteiros positivos* a *e* b *possuem as fatorações*

$$a = \prod_{i=1}^{\infty} p_i^{a_i}, \ b = \prod_{i=1}^{\infty} p_i^{b_i}$$

então o máximo divisor comum de a *e* b *é igual a:*

$$(a, b) = \prod_{i=1}^{\infty} p_i^{c_i}$$

onde $c_i = \min\{a_i, b_i\}$.

Demonstração: Para que um produto de fatores primos comuns seja um divisor comum nenhum expoente c_i de p_i poderá superar nem a_i e nem b_i. Como estamos interessados no maior dos divisores positivos, basta tomarmos, para c_i, o menor desses dois. □

Teorema 1.12. (Euclides) *A seqüência dos números primos é infinita.*

Demonstração: Vamos supor que a seqüência dos primos seja finita. Seja pois, $p_1, p_2, \ldots, p_n$ a lista de todos os primos. Consideramos o número $R = p_1.p_2 \ldots p_n + 1$. É claro que R não é divisível por nenhum dos p_i de nossa lista e que R é maior do que qualquer p_i. Mas, pelo Teorema 1.9, ou R é primo ou possui algum fator primo e isto implica na existência de um primo que não pertence à nossa lista. Portanto a seqüência dos números primos não pode ser finita. □

Teorema 1.13. *Para qualquer inteiro positivo* k, *existem* k *inteiros consecutivos todos compostos. Em outras palavras, existem "saltos" arbitrariamente grandes na seqüência dos números primos.*

Demonstração: Para demonstrarmos este resultado observamos que como $(k+1)!$ é divisível por todos os k números entre 2 e $k+1$, então a seqüência

$$(k+1)! + 2, (k+1)! + 3, \ldots, (k+1)! + k, (k+1)! + (k+1)$$

é, toda ela, composta por k números consecutivos compostos, concluíndo a demonstração. □

Na demonstração do próximo teorema faremos uso do fato de que os números definidos por

$$\binom{n}{k} = \frac{n!}{k!(n-k)!},$$

onde n e k são inteiros não negativos com $k \le n$, são inteiros. Este fato está demonstrado no Capítulo 4 (Teorema 4.10), mas pode, também, ser provado por indução uma vez que

$$\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1} \tag{1.3}$$

Esta simples e importante equação que pode ser provada através de argumento combinatório (ver [29] p. 262) segue, facilmente, como mostrado a seguir

$$\binom{n}{k} + \binom{n}{k-1} = \frac{n!}{k!(n-k)!} + \frac{n!}{(k-1)!(n-k+1)!}$$
$$= \frac{n!(n+1-k)}{k!(n+1-k)!} + \frac{n!k}{k!(n+1-k)!}$$

$$= \frac{(n+1)!}{k!(n+1-k)!} = \binom{n+1}{k}.$$

Teorema 1.14. *O produto de qualquer seqüência de* k *inteiros consecutivos é divisível por* $k!$.

Demonstração: Vamos considerar n e k inteiros positivos com $k \leq n$. Sabemos que o número de combinações de n, tomadas k a k, é um inteiro dado por:

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{n(n-1)\dots(n-k+1)}{k!}$$

Sendo o numerador o produto de k inteiros consecutivos temos o resultado para uma seqüência de k inteiros positivos. No caso de zero ser um elemento na seqüência o resultado é trivial, uma vez que zero é divisível por qualquer número.

Se a seqüência contiver só números negativos, a fração do lado direito da igualdade acima sofrerá, no máximo, uma mudança de sinal continuando a ser um inteiro, o que conclui nossa demonstração. □

Teorema 1.15 *Se* n *não é primo, então* n *possui, necessariamente, um fator primo menor do que ou igual a* $\sqrt{n}$.

Demonstração: Sendo n composto então $n = n_1 \cdot n_2$ onde $1 < n_1 < n$, $1 < n_2 < n$. Sem perda de generalidade vamos supor $n_1 \leq n_2$. Logo n_1 tem que ser $\leq \sqrt{n}$ pois, caso contrário, teríamos $n = n_1.n_2 > \sqrt{n}.\sqrt{n} = n$ o que é absurdo. Logo, como pelo Teorema 1.9, n_1 possui algum fator primo p, este deve ser $\leq \sqrt{n}$. Como p, sendo um fator primo de n_1 é também um fator de n, a demonstração está completa. □

Este resultado tem uma importante aplicação prática. Ele nos diz que, para testarmos se um número é primo, é suficiente testarmos divisibilidade apenas pelos primos $\leq \sqrt{n}$. Portanto, se desejarmos obter a lista de todos os primos menores que 60 devemos excluir dentre os números de 2 a 60 aqueles que são múltiplos de 2, 3, 5 e 7 pois estes são os primos $\leq \sqrt{60}$. Este processo é chamado de crivo de Eratóstenes.

	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~

Logo, os primos entre 2 e 60 são todos aqueles que não foram eliminados pelo processo descrito, isto é,

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59.

1.7 Mínimo Múltiplo Comum

Definição 1.4 O *Mínimo múltiplo comum* de dois inteiros positivos a e b é o menor inteiro positivo que é divisível por a e b. Vamos denotá-lo por $[a, b]$.

Proposição 1.5 *Se* $a = p_1^{a_1} p_2^{a_2} p_3^{a_3} \cdots p_n^{a_n}$ *e* $b = p_1^{b_1} p_2^{b_2} p_3^{b_3} \cdots p_n^{b_n}$ *onde* $p_1, p_2, \dots, p_n$ *são os primos que ocorrem nas fatorações de* a *e* b, *então*

$$[a, b] = p_1^{\max\{a_1, b_1\}} p_2^{\max\{a_2, b_2\}} \cdots p_n^{\max\{a_n, b_n\}}.$$

Demonstração: Da definição de mínimo múltiplo comum nenhum fator primo p_i deste mínimo poderá ter um expoente que seja inferior nem a a_i e nem a b_i. Se tomarmos, pois, o maior destes dois para expoente de p_i teremos, não apenas um múltiplo comum, mas o menor possível dentre todos eles. O que conclui a demonstração. □

Proposição 1.6 *Se* x *e* y *são números reais então*

$$\max\{x, y\} + \min\{x, y\} = x + y.$$

Demonstração: Se $x = y$ então o $\max\{x, y\} = \min\{x, y\} = x = y$ e o resultado se verifica trivialmente. Sem perda de generalidade podemos supor $x < y$. Então $\max\{x, y\} = y$ e $\min\{x, y\} = x$, o que conclui a demonstração. □

Teorema 1.16 *Para* a *e* b *inteiros positivos temos,* $[a, b] \cdot (a, b) = a \cdot b$.

Demonstração: Vamos supor que a e b tenham fatorações dadas na Proposição 1.5. Do Teorema 1.11 temos que,

$$(a, b) = \prod_{i=1}^{n} p_i^{\min\{a_i, b_i\}}.$$

e, da Proposição 1.5, que

$$[a, b] = \prod_{i=1}^{n} p_i^{\max\{a_i, b_i\}}.$$

Agora, pela proposição anterior, o resultado segue imediatamente. □

Proposição 1.7 *Sejam* a *e* b *inteiros positivos relativamente primos entre si. Então se* d *é divisior positivo de* ab, *existe um único par de divisores positivos* d_1 *de* a *e* d_2 *de* b *tais que* $d = d_1 d_2$. *Reciprocamente, se* d_1 *e* d_2 *são divisores positivos de* a *e* b, *respectivamente, então* $d = d_1 d_2$ *é um divisor positivo de* ab.

Demonstração: Consideremos as fatorações de a e b dadas por

$$a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n} \quad \text{e} \quad b = q_1^{b_1} q_2^{b_2} \cdots q_m^{b_m}.$$

Como $(a, b) = 1$ os conjuntos $\{p_1, p_2, \ldots, p_n\}$ e $\{q_1, q_2, \ldots, q_m\}$ são disjuntos. Isto nos diz que a fatoração de ab é dada por

$$ab = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n} q_1^{b_1} q_2^{b_2} \cdots q_m^{b_m}.$$

Portanto, se d é um divisor positivo de ab, então

$$d = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n} q_1^{\beta_1} q_2^{\beta_2} \cdots q_m^{\beta_m}$$

$$0 \leq \alpha_i \leq a_i, \ i = 1, 2, \ldots, n \quad \text{e} \quad 0 \leq \beta_j \leq b_j, \ j = 1, 2, \ldots, m.$$

Definimos

$$d_1 = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n} \quad \text{e} \quad d_2 = q_1^{\beta_1} q_2^{\beta_2} \cdots q_m^{\beta_m}.$$

É óbvio que $(d_1, d_2) = 1$ e $d_1 d_2 = d$. Para demonstrarmos a recíproca consideramos d_1 e d_2 como divisores positivos de a e b, respectivamente. Logo,

$$d_1 = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}, \quad 0 \leq \alpha_i \leq a_i, \ i = 1, 2, \ldots, n$$

e

$$d_2 = q_1^{\beta_1} q_2^{\beta_2} \cdots q_m^{\beta_m}, \quad 0 \leq \beta_j \leq b_j, \ j = 1, 2, \ldots, m.$$

É claro que o número

$$d = d_1 d_2 = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_n^{\alpha_n} q_1^{\beta_1} q_2^{\beta_2} \ldots q_m^{\beta_m}$$

é um divisor de ab. □

Antes de demonstrarmos o próximo teorema vamos descrever, através de um exemplo, a idéia utilizada na demonstração, da mesma forma como fizemos antes do Teorema 1.8.

Queremos representar o número 53742 na base 7. Para explicar melhor o que queremos fazer vamos, primeiramente, recordar alguns fatos familiares

sobre representação na base 10. Para isto consideramos o número 50341. Aqui temos 1 unidade, 4 dezenas, 3 centenas e 5 dezenas de milhar. O zero na posição dos "milhares" nos fala da ausência da potência terceira de 10. Como sabemos, isto costuma ser escrito da seguinte forma:

$$5 \times 10^4 + 0 \times 10^3 + 3 \times 10^2 + 4 \times 10 + 1.$$

A expressão acima nos diz que a maior potência de 10 menor do que ou igual a 50341 é 10^4. Nos diz, também, que se dividirmos 50341 por 10^4 vamos encontrar um quociente igual a 5 e um resto inferior a 10^3, por causa do "0×10^3". Que este resto é maior que 10^2 e que, quando dividido por 10^2 dá um quociente 3 e resto superior a 10. E, finalmente, que este último resto, quando dividido por 10 dá quociente 4 e resto 1. Para expressarmos 53742 na base 7 vamos proceder de forma a obter informações semelhantes a estas, onde 7 irá representar o papel do "10" no que acabamos de descrever. Primeiro dividímos 53742 por 7 obtendo quociente 7677 e resto 3. Em seguida dividimos este quociente 7677 por 7 obtendo um segundo quociente igual a 1096 e resto 5, em seguida repetimos este procedimento até chegarmos a um quociente nulo, obtendo a seguinte seqüência de igualdades:

$$\begin{aligned}
53742 &= 7 \times 7677 + 3 \\
7677 &= 7 \times 1096 + 5 \\
1096 &= 7 \times 156 + 4 \\
156 &= 7 \times 22 + 2 \\
22 &= 7 \times 3 + 1 \\
3 &= 7 \times 0 + 3.
\end{aligned}$$

Como a seqüência dos quocientes é decrescente e formada somente por inteiros positivos ela deve atingir o valor zero. Na primeira destas equações substituímos o valor de 7677 dado na segunda. Na expressão resultante substituímos o valor de 1096 dado na terceira, nesta o valor de 156 dado na quarta e assim sucessivamente obtendo a seguinte expressão:

$$\begin{aligned}
53742 &= 7(7 \times 1096 + 5) + 3 \\
&= 7^2 \times 1096 + 5 \times 7 + 3 \\
&= 7^2(7 \times 156 + 4) + 5 \times 7 + 3 \\
&= 7^3 \times 156 + 4 \times 7^2 + 5 \times 7 + 3 \\
&= 7^3(7 \times 22 + 2) + 4 \times 7^2 + 5 \times 7 + 3 \\
&= 7^4 \times 22 + 2 \times 7^3 + 4 \times 7^2 + 5 \times 7 + 3
\end{aligned}$$

$$= 7^4(7 \times 3 + 1) + 2 \times 7^3 + 4 \times 7^2 + 5 \times 7 + 3$$
$$= 3 \times 7^5 + 1 \times 7^4 + 2 \times 7^3 + 4 \times 7^2 + 5 \times 7 + 3.$$

Dizemos ser, esta expressão, a representação do número 53742 na base 7 que denotamos por $(312453)_7$. Agora ficará mais fácil a demonstração do teorema que se segue.

Teorema 1.17 *Seja* b *um inteiro positivo maior do que 1. Então todo inteiro positivo* n *pode ser representado de maneira única da seguinte forma:*

$$n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0. \tag{1.4}$$

onde $k \geq 0, a_k \neq 0$ *e* $0 \leq a_i < b,\ i = 0, 1, 2, \ldots, k.$

Primeira demonstração: Para mostrarmos a existência procedemos exatamente da forma como acabamos de fazer para o caso $b = 7$. Iniciamos pela divisão de n por b obtendo quociente q_0 e resto a_0. Em seguida dividimos q_0 por b obtendo quociente q_1 e resto a_1, e, prosseguindo desta forma, obtemos a seguinte seqüência de igualdades:

$$\begin{aligned} n &= bq_0 + a_0 \\ q_0 &= bq_1 + a_1 \\ q_1 &= bq_2 + a_2 \\ q_2 &= bq_3 + a_3 \\ &\vdots \\ q_{k-2} &= bq_{k-1} + a_{k-1} \\ q_{k-1} &= b \cdot 0 + a_k, \end{aligned}$$

onde $0 \leq a_j < b,\ \ j = 0, 1, 2, \ldots, k.$

Agora, na primeira destas equações, substituímos o valor de q_0 dado na segunda. Em seguida substituímos, nesta expressão, o valor de q_1 dado na terceira, e assim sucessivamente, obtendo:

$$\begin{aligned} n &= bq_0 + a_0 \\ &= b(bq_1 + a_1) + a_0 \\ &= b^2 q_1 + a_1 b + a_0 \\ &= b^2(bq_2 + a_2) + a_1 b + a_0 \\ &= b^3 q_2 + a_2 b^2 + a_1 b + a_0 \\ &= b^3(bq_3 + a_3) + a_2 b^2 + a_1 b + a_0 \\ &= b^4 q_3 + a_3 b^3 + a_2 b^2 + a_1 b + a_0 \end{aligned}$$

$$\begin{aligned} &\vdots \\ &= b^k q_{k-1} + a_{k-1} b^{k-1} + \ldots + a_2 b^2 + a_1 b + a_0 \\ &= a_k b^k + a_{k-1} b^{k-1} + \ldots + a_1 b + a_0. \end{aligned}$$

Nos resta mostrar, agora, a unicidade desta representação.

Vamos denotar por $d_b(n)$ o número de representações de n na base b. Queremos, portanto, mostrar que $d_b(n)$ é sempre igual a 1. Como alguns dos coeficientes a_j podem ser nulos podemos supor, excluindo tais termos, que n possa ser representado na forma

$$n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_s b^s$$

onde a_k e a_s são não nulos. Logo

$$\begin{aligned} n - 1 &= a_k b^k + a_{k-1} b^{k-1} + \ldots + a_s b^s - 1 \\ &= a_k b^k + a_{k-1} b^{k-1} + \ldots + (a_s - 1) b^s + b^s - 1 \\ &= a_k b^k + a_{k-1} b^{k-1} + \ldots + (a_s - 1) b^s + (b - 1) \sum_{j=0}^{s-1} b^j, \end{aligned}$$

uma vez que $b^s - 1 = (b-1) \sum_{j=0}^{s-1} b^j$.

Isto nos diz que para cada representação de n na base b é possível encontrar uma representação, na base b, para $n - 1$. Logo $d_b(n) \leq d_b(n-1)$. Esta desigualdade nos diz que para $m \geq n$, temos

$$d_b(m) \leq d_b(m-1) \leq d_b(m-2) \leq \ldots \leq d_b(n+1) \leq d_b(n).$$

Logo, como $n > 1$ e $d_b(n) \geq 1$, obtemos $1 \leq d_b(n) \leq d_b(1) = 1$. Esta última série de desigualdades nos garante que $d_b(n) = 1$, o que conclui a demonstração. □

Segunda demonstração: Usamos indução em n. Para $n = 1$ tomamos $k = 0$ e $a_0 = 1$. Portanto (1.4), é verdadeira para $n = 1$.

Assumimos que o teorema seja válido para todo inteiro menor do que n. Como $b > 1, n > 0, n$ se encontra entre dois números consecutivos da seguinte seqüência:

$$b^0, b^1, b^2, \ldots, b^k, \ldots$$

Explicitamente, existe um único inteiro k, tal que $b^k \leq n < b^{k+1}$. Pelo teorema (1.2) temos

$$n = a_k b^k + r, \quad 0 \leq r < b^k.$$

Claramente $0 < a_k < b$. Se $r = 0$, então

$$n = a_k b^k + 0.b^{k-1} + \cdots + 0.b + 0.$$

Se $r \neq 0$, pela hipótese de indução

$$r = c_t b^t + \cdots + c_1 b + c_0, \quad t < k$$

onde $0 \leq c_i < b$. Desta forma

$$n = a_k b^k + c_t b^t + \cdots + c_1 b + c_0$$

e (1.4) se verifica.

Para provarmos a unicidade, assumimos a existência de uma outra representação

$$n = d_m b^m + \cdots + d_1 b + d_0 \tag{1.5}$$

com $m \geq 0, d_m \neq 0$ e $0 \leq d_i < b$. Se a_i e d_i não são todos iguais, pela subtração membro a membro, de (1.4) da equação (1.5) obtemos:

$$0 = h_s b^s + \cdots + h_1 b + h_0$$

onde s é o maior valor de i para os quais $a_i \neq d_i$. Logo, $h_s \neq 0$. Se $s = 0$, temos uma contradição pois estamos assumindo que (1.5) seja diferente de (1.4). Se $s > 0$, temos

$$|h_i| = |a_i - d_i| \leq b - 1, \ i = 0, \ldots, s-1,$$
$$h_s b^s = -(h_{s-1} b^{s-1} + \cdots + h_0)$$

e, portanto

$$\begin{aligned} b^s \leq |h_s b^s| &= |h_{s-1} b^{s-1} + \cdots + h_0| \\ &\leq (b-1)(b^{s-1} + \cdots + b + 1) = b^s - 1 \end{aligned}$$

o que é, também, uma contradição. Desta forma concluímos que os $a_i's$ e $d_i's$ são todos iguais, isto é, $k = m, \quad a_i = d_i, \quad i = 0, 1, \ldots, k$, e a representação é única. □

Definição 1.5 Um número da forma

$$F_n = 2^{2^n} + 1$$

é chamado de *número de Fermat.* O teorema seguinte nos fornece uma segunda prova da infinitude dos números primos.

Teorema 1.18 *Quaisquer dois números de Fermat distintos F_n e F_m são relativamente primos.*

Demonstração: Para provarmos este resultado vamos mostrar, primeiramente, que a seguinte relação se verifica

$$F_0 F_1 \cdots F_{n-1} = F_n - 2.$$

A prova é por indução. Como o caso $n = 1$ se verifica, isto é, $F_0 = F_1 - 2$, vamos supor a validade para n e mostrar que a mesma relação também vale para $n + 1$.

$$\begin{aligned} F_0 F_1 \cdots F_n &= (F_0 F_1 \cdots F_{n-1}) F_n \\ &= (F_n - 2) F_n \\ &= (2^{2^n} + 1 - 2)(2^{2^n} + 1) \\ &= (2^{2^n} - 1)(2^{2^n} + 1) = 2^{2^{n+1}} - 1 \\ &= 2^{2^{n+1}} + 1 - 2 = F_{n+1} - 2. \end{aligned}$$

Supondo $n < m$ temos, pela relação acima, que

$$F_0 F_1 F_2 \cdots F_n \cdots F_{m-1} = F_m - 2$$

o que implica que $F_m - F_0 \cdots F_n \cdots F_{m-1} = 2$. Logo, se um número d divide F_n e F_m então d divide 2. Como F_n é ímpar d não pode ser 2 e portanto $(F_n, F_m) = 1$. □

Deste fato podemos concluir que existem infinitos números primos, pois sendo infinita a seqüência dos números de Fermat e não possuindo fatores primos em comum, isto não poderia ocorrer caso este conjunto fosse finito.

Teorema 1.19 *Existem infinitos primos da forma* $6k + 5$.

Demonstração: Pelo Algoritmo da Divisão quando dividimos um número qualquer por 6, os possíveis restos são 0, 1, 2, 3, 4 e 5 o que significa que um inteiro pode ser escrito em uma das seguintes formas: $6k, 6k+1, 6k+2, 6k+3, 6k+4, 6k+5$. Logo, se p é primo ímpar, então p é da forma $6k+1$ ou

$6k+5$. Para mostrarmos que existem infinitos primos de forma $6k+5$ vamos supor o contrário, isto é, que existe apenas um número finito deles. Sejam $p_0 = 5, p_1, p_2, \ldots, p_r$ estes números. Considerernos o número

$$P = 6p_1p_2\cdots p_r + 5.$$

É claro que, pela Proposição 1.2, este número não é divisível por nenhum dos primos $p_0, p_1, p_2, \ldots, p_r$. Afirmamos que P possui um fator primo da forma $6k+5$, pois, caso contrário todos seriam da forma $6k+1$, o que não é possível, uma vez que o produto de dois números da forma $6k+1$ é sempre desta mesma forma. Isto mostra que, ou P é primo, ou P possui um fator primo da forma $6k+5$, ficando provada a existência de infinitos primos da forma $6k+5$. □

O que acabamos de demonstrar é um caso especial de um importante teorema de Dirichlet chamado "Teorema dos Primos em Progressão Aritmética" que diz: Se a e b são inteiros relativamente primos então a progressão aritmética $an+b$, $n = 1, 2, 3, \ldots$ contém um número infinito de primos.

1.8 Critérios de Divisibilidade

Começamos com o critério de divisibilidade por 3. Os critérios que apresentamos são, basicamente, aplicações da Proposição 1.2.

Vamos, para descrever a idéia, considerar um número n com 5 dígitos $abcde$. Como estamos considerando a representação dele na base 10, ele pode ser escrito na forma:

$$n = a\times 10^4 + b\times 10^3 + c\times 10^2 + d\times 10 + e.$$

Fazemos, a seguir as seguintes substituições:

$$\begin{aligned} 10 &= 9+1 \\ 100 &= 99+1 \\ 1000 &= 999+1 \\ 10000 &= 9999+1 \end{aligned}$$

obtendo:

$$\begin{aligned} n &= a(9999+1) + b(999+1) + c(99+1) + d(9+1) + e \\ &= (9999a + 999b + 99c + 9d) + (a+b+c+d+e) \\ &= 9(1111a + 111b + 11c + d) + (a+b+c+d+e). \end{aligned}$$

Disto concluímos que se $3|n$, então como $3|9(1111a + 111b + 11c + d)$, pela Proposição 1.2, 3 deve dividir $(a+b+c+d+e)$. Reciprocamente, se $3|(a+b+c+d+e)$, então $3|n$, uma vez que $3|9(1111a + 111b + 11c + d)$.

Provamos, desta maneira, o seguinte critério de divisibilidade por 3: "Um número é divisível por 3 se, e somente se, a soma de seus dígitos é divisível por 3."

Para obter um critério de divisibilidade por 9 basta, no argumento acima, substituir 3 por 9, concluindo o seguinte: "Um número é divisível por 9 se, e somente se, a soma de seus dígitos é divisível por 9."

Exemplo 1.7: 4578 é divisível por 3 pois, $(4+5+7+8) = 24$ é divisível por 3.

Exemplo 1.8: 4578 não é divisível por 9 pois, $(4+5+7+8) = 24$ não é divisível por 9.

Como todo número inteiro pode ser escrito na forma $10k+j$, onde j é o dígito das unidades, e como 10 é divisível por 2, então ele será divisível por 2 se, e somente se, j for múltiplo de dois. Em outras palavras se, e somente se, ele for par.

O critério de divisibilidade por 4 se obtém considerando-se o número na forma $100k+ab$ onde "ab"é o número formado pelos dois últimos dígitos, isto é, o das dezenas e o da unidade e observando ser 100 um múltiplo de 4.

Exemplo 1.9: 72548 é divisível por 4 pois, 48 é múltiplo de 4. Como 14 não é divisível por 4, então 73514 não é divisível por 4.

Discutimos, agora, os critérios de divisibilidade por 7 e 11. Iniciamos com 7. Para descrever o critério consideramos um exemplo. Seja $n = 59325$. Separamos o dígito 5 das unidades e do número restante 5932, subtraímos o dobro deste dígito, isto é

$$\begin{array}{r} 5932 \\ -10 \\ \hline 5922 \end{array}$$

Em seguida repetimos este procedimento até a obtenção de um número suficientemente pequeno que possamos reconhecer, facilmente, se é ou não divisível por 7.

$$\begin{array}{r} 592 \\ -4 \\ \hline 588 \end{array} \qquad \begin{array}{r} 58 \\ -16 \\ \hline 42 \end{array}$$

Como 42 é divisível por 7, o critério que vamos provar é que este fato irá implicar que o número original também deverá ser divisível por 7.

Seja i o dígito das unidades do número n, então n pode ser escrito como $10k+i$. (No exemplo acima $k = 5932$ e $i = 5$). No procedimento descrito acima obtivemos um número r como sendo $k - 2i$. Feitas estas observações,

será suficiente provar que os números $10k + i$ e $k - 2i$ são tais que, se um deles é múltiplo de 7, o outro também é. Isto é, devemos provar a seguinte equivalência:

$$10k + i \text{ é múltiplo de } 7 \Leftrightarrow k - 2i \text{ é múltiplo de } 7.$$

Demonstração: ($\Rightarrow$) Se $10k + i$ é múltiplo de 7, então existe um inteiro m tal que $10k + i = 7m$ e, portanto, $k - 2i = k - 2(7m - 10k) = k - 14m + 20k = 21k - 14m = 7(3k - 2m)$ o que implica $k - 2i$ ser múltiplo de 7.

($\Leftarrow$) Se $k - 2i$ é múltiplo de 7, então existe um inteiro n, tal que $k - 2i = 7n$ e, portanto, $10k + i = 10(7n + 2i) + i = 70n + 20i + i = 70n + 21i = 7(10n + 3i)$ o que implica $10k + i$ ser múltiplo de 7. Isto conclui a prova.

No exemplo acima, como 42 é divisível por 7, então 588 também é. Sendo 588 divisível por 7, então 5932 também deverá ser e, a divisibilidade deste por 7 implica que 59325 deverá ser divisível por 7.

Vamos olhar mais um exemplo. Seja $n = 735421$. Procedendo da maneira descrita, obtemos:

$$\begin{aligned} 73542 - 2 \times 1 &= 73540 \\ 7354 - 2 \times 0 &= 7354 \\ 735 - 2 \times 4 &= 727 \\ 72 - 2 \times 7 &= 58 \end{aligned}$$

como $7 \nmid 58$, então $7 \nmid 735421$.

Para a descrição do critério de divisibilidade por 11, também utilizaremos um exemplo. Seja n um número de 5 dígitos **abcde**. Como sabemos este pode ser representado como

$$n = a \times 10^4 + b \times 10^3 + c \times 10^2 + d \times 10 + e.$$

Fazendo as seguintes substituições

$$\begin{aligned} 10 &= 11 - 1 \\ 100 &= 99 + 1 \\ 1000 &= 1001 - 1 \\ 10000 &= 9999 + 1 \end{aligned}$$

obtemos

$$a(9999 + 1) + b(1001 - 1) + c(99 + 1) + d(11 - 1) + e = \\ 9999a + 1001b + 99c + 11d + [(a + c + e) - (b + d)].$$

Como $9999a + 1001b + 99c + 11d$ é divisível por 11, então n será divisível por 11, se, e somente se, $[(a + c + e) - (b + d)]$ o for. Observe que os dígitos a, c e e ocupam posições ímpares em **abcde** enquanto b e d posições pares. Nesta última sentença, utilizamos dois fatos elementares:

i) todo número da forma $99\ldots9$, onde o número de "9"s é par, é divisível por 11.

ii) Todo número da forma $100\ldots01$, onde o número de "0"s entre os dois "uns"é par, também é múltiplo de 11. Para a prova observe que $9999 = 9900 + 99$; $999999 = 999900 + 99, \ldots$, e que $1001 = 990 + 11$; $100001 = 99990 + 11, \ldots$. □

No próximo capítulo mostraremos um critério que serve, ao mesmo tempo, para testar a divisibilidade por 7, 11 e 13.

O assunto discutido neste capítulo é extremamente rico em resultados interessantes. Com a finalidade de ilustrar apenas alguns destes resultados, apresentamos a seguir, através de problemas resolvidos, alguns resultados de interesse.

1.9 Problemas Resolvidos

Problema 1.1 Se a e b são inteiros diferentes, então existe um número infinito de inteiros n tais que $a + n$ e $b + n$ são relativamente primos.

Solução: Suponhamos $a < b$. Se escolhermos k positivo e suficientemente grande, o número $n = (b - a)k + 1 - a$ será positivo. Como $a + n = (b - a)k + 1$ e $b + n = (b - a)(k + 1) + 1$, então $a + n$ e $b + n$ são positivos. Se $d | (a + n)$ e $d | (b + n)$ então $d | (b - a)$, e como $a + n = (b - a)k + 1$ temos pela Proposição 1.2 que $d | 1$. Logo $(a + n, b + n) = 1$. Como qualquer k, maior do que este escolhido acima, irá fornecer um n com a propriedade desejada, a seqüência dos n's é infinita. □

Problema 1.2 Existe uma seqüência infinita de números triangulares , isto é, números da forma $t_n = n(n + 1)/2$, $n = 1, 2, \ldots$ que são, dois a dois, relativamente primos.

Solução: Mostramos que, se para algum inteiro n, temos n números triangulares $a_1 < a_2 < \ldots < a_n$ os quais são relativamente primos, então existe um número triangular $t > a_n$, tal que $(t, a_1, a_2, \ldots, a_n) = 1$. Seja $a = a_1.a_2.\cdots.a_n$. Os números $a + 1$ e $2a + 1$ são relativamente primos com a e o número

$$a_{n+1} = \frac{(2a + 1)(2a + 2)}{2} = (a + 1)(2a + 1)$$

é um número triangular maior do que a_n. Como $(a_{n+1}, a) = 1$, a_{n+1} é relativamente primo com todos os números $a_1, a_2, \ldots, a_n$. Isto mostra que sempre será possível acrescentar um novo número triangular que seja relativamente primo com todos os anteriores e desta forma gerarmos a seqüência infinita desejada. □

Observação: O nome "números triangulares" vem do fato de serem, estes, os números de pontos na seqüência de figuras.

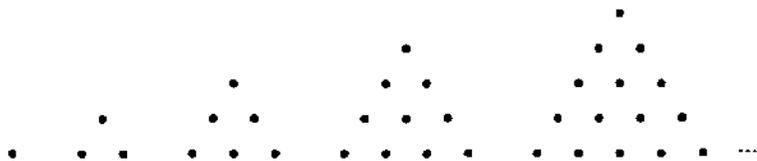



Figura 1.1

Problema 1.3 Para $n \geq 2$ e k um inteiro positivo qualquer temos que $(n-1) | (n^k - 1)$.

Solução: Este resultado é uma conseqüência imediata da igualdade:

$$n^k - 1 = (n-1)\,(n^{k-1} + n^{k-2} + \cdots + n^2 + n + 1).$$

Problema 1.4 Para a, m e n inteiros positivos com $m \neq n$, temos que

$$(a^{2^m} + 1, a^{2^n} + 1) = \begin{cases} 1 \text{ se } a \text{ é par} \\ 2 \text{ se } a \text{ é ímpar} \end{cases}$$

Solução: Se tomarmos, aqui, $a = 2$ teremos o resultado, já demonstrado (Teorema 1.18), a respeito dos números de Fermat. Utilizamos, na demonstração, a seguinte relação

$$A_0 A_1 \cdots A_{n-1} = \frac{A_n - 2}{a - 1}$$

onde $A_n = a^{2^n} + 1$ e a é um inteiro, $a \geq 2$. Observe que, isto também, é uma generalização do resultado usado na demonstração do Teorema 1.18. Aqui, também, usamos indução. Para $n = 1$ temos $A_0 = (A_1 - 2)/(a-1)$. Vamos supor que a relação seja válida para todo m menor do que ou igual a $n - 1$ e provar que ela também se verifica para n. Com esta hipótese temos:

$$A_0 A_1 \cdots A_n = (A_0 A_1 \cdots A_{n-1}) A_n$$

$$\begin{aligned}
&= \left(\frac{A_n - 2}{a - 1}\right) A_n = \frac{(a^{2^n} + 1 - 2)}{a - 1} \cdot (a^{2^n} + 1) \\
&= \frac{(a^{2^n} - 1)\,(a^{2^n} + 1)}{a - 1} = \frac{a^{2^{n+1}} - 1}{a - 1} \\
&= \frac{a^{2^{n+1}} + 1 - 2}{a - 1} = \frac{A_{n+1} - 2}{a - 1}
\end{aligned}$$

o que mostra, pela segunda forma do princípio de indução finita que

$$A_0 A_1 \cdots A_{n-1} = \frac{A_n - 2}{a - 1}$$

é válida para todo $n \geq 1$. Logo, para $m < n$ temos

$$A_n - (a-1)\,(A_0 A_1 \cdots A_m \cdots A_{n-1}) = 2$$

isto mostra que se d for um divisor comum de A_n e A_m então $d = 1$ ou $d = 2$. Mas A_n é ímpar para "a"par e par para "a"ímpar. Portanto $d = 1$ para "a"par e $d = 2$ para "a"ímpar, o que conclui a demonstração.

Problema 1.5 Para todo inteiro $n > 1$ a soma $\sum_{j=1}^{n} \frac{1}{j}$ nunca é um número inteiro.

Solução: Consideramos S o conjunto dos inteiros $1, 2, 3, \ldots, n$. Seja 2^k a maior potência de 2 em S. Provamos, primeiramente, que 2^k não divide nenhum outro inteiro em S. Se 2^k for um divisor de algum outro inteiro em S além dele mesmo, este inteiro será da forma $b2^k$, onde $b > 1$. Logo 2^{k+1} estará também em S, o que contradiz a definição de k. Vamos supor que a soma dada seja um inteiro t. É claro que o mínimo múltiplo comum dos elementos de S é da forma $m2^k$, onde m é ímpar. Multiplicando-se esta soma por $m2^{k-1}$, temos:

$$m \cdot 2^{k-1} \cdot \sum_{j=1}^{n} \frac{1}{j} = m \cdot t \cdot 2^{k-1}.$$

Quando multiplicamos cada termo da soma por $m2^{k-1}$, um dos termos será $m/2$ e todos os outros serão inteiros, o que é uma contradição. (Lembre-se que m é ímpar). □

Problema 1.6 Se $m > n$ então $(a^{2^n} + 1) | (a^{2^m} - 1)$.

Solução: Na seqüência

$$x + 1, x^2 - 1, x^4 - 1, x^8 - 1, x^{16} - 1, \ldots, x^{2^n} - 1, \ldots$$

cada termo divide o seguinte. Basta tomarmos $x = a^{2^n}$ que teremos o resultado desejado.

Problema 1.7 Se a e b são ímpares, então $a^2 + b^2$ não pode ser um quadrado perfeito.

Solução: Como a e b são ímpares, existem inteiros t e s tais que: $a = 2t + 1$ e $b = 2s + 1$. Logo

$$\begin{aligned} a^2 + b^2 &= (2t+1)^2 + (2s+1)^2 \\ &= 4(t^2 + s^2 + t + s) + 2 \\ &= 2(2k+1), \\ k &= t^2 + s^2 + t + s. \end{aligned}$$

Portanto $a^2 + b^2$ é um número par não divisível por 4 e desta forma não pode ser um quadrado perfeito pois se $2|c^2$, então $2|c$, o que implica $4|c^2$. □

Este resultado nos diz que, num triângulo retângulo com lados inteiros, os dois catetos não podem ser ambos ímpares.

Problema 1.8 Se a e n são inteiros, com pelo menos um não-nulo, então $(a, a+n)|n$ para todo inteiro n.

Solução: Isto é uma conseqüência imediata do Teorema 1.5 bastando escolher $b = a + n$ e $x = -1$.

Problema 1.9 Mostre que $(n-1)^2|(n^k - 1) \Leftrightarrow (n-1)|k$.

Solução: Consideramos a seguinte identidade:

$$n^k - 1 = (n-1)^k + \binom{k}{1}(n-1)^{k-1} + \binom{k}{2}(n-1)^{k-2} + \cdots + \binom{k}{k-2}(n-1)^2 + k(n-1).$$

Onde usamos o fato de

$$\begin{aligned} n^k &= ((n-1)+1)^k \\ &= (n-1)^k + \binom{k}{1}(n-1)^{k-1} + \binom{k}{2}(n-1)^{k-2} + \cdots + \\ &\quad + \binom{k}{k-2}(n-1)^2 + k(n-1) + 1. \end{aligned}$$

É fácil observar que

$$A = (n-1)^k + \binom{k}{1}(n-1)^{k-1} + \binom{k}{2}(n-1)^{k-2} + \cdots \binom{k}{k-2}(n-1)^2$$

é divisível por $(n-1)^2$ pois todos os termos desta soma possuem $(n-1)^2$ como fator. Disto concluimos que se $(n-1)^2|(n^k-1)$, então $n^k - 1 - A = k(n-1)$ é divisível por $(n-1)^2$ o que implica $(n-1)|k$. A recíproca é também imediata pois se $(n-1)|k$, então $(n-1)^2|k(n-1)$ o que implica $(n-1)^2|(n^k-1)$, uma vez que A é divisível por $(n-1)^2$, o que conclui a nossa demonstração. □

Problema 1.10 Mostre que se m e n são inteiros positivos com $m > 1$, então $n < m^n$.

Solução: Sabemos que

$$n = \underbrace{1 + 1 + \cdots + 1}_{n-\text{termos}} \le 1 + m + m^2 + \ldots + m^{n-1} = \frac{m^n - 1}{m - 1}.$$

Mas $\dfrac{m^n - 1}{m-1} \le m^n - 1 < m^n$. Logo, $n < m^n$. □

Problema 1.11 Mostrar que todo inteiro positivo pode ser escrito como a soma de números de Fibonacci distintos. (ver problema 13 no final do capítulo)

Solução: Sejam k um inteiro positivo e $F_1, F_2, \ldots, F_n, \ldots$ a seqüência de Fibonacci. Se k não pertence à seqüência seja n tal que $F_{n-1} < k < F_n$. Logo $0 < k - F_{n-1} < F_n - F_{n-1} = F_{n-2}$. Por indução vamos supor que o resultado se verifica para todo inteiro menor do que k. Se k for um elemento da seqüência a indução está completa. Se ele não pertence à seqüência então, como vimos acima, existe n tal que $k - F_{n-1} < F_{n-2}$ e, portanto, $k - F_{n-1}$ pode ser expresso como a soma de termos da seqüência $F_1, F_2, \ldots, F_{n-3}$ o que completa a demonstração. □

Problema 1.12 Mostrar que $(n! + 1, (n+1)! + 1) = 1$.

Solução: Seja p primo um divisor comum de $n! + 1$ e $(n+1)! + 1$. Logo p divide a diferença destes números que é

$$(n+1)! + 1 - (n! + 1) = n.n!$$

o que implica $p|n!$. Como $p|(n! + 1)$, $p|(n! + 1 - n!)$ e, portanto, $p = 1$ (contradição). □

Problema 1.13 Mostrar que se a e b são inteiros com $(a, b) = 1$, então $(a + b, a - b) = 1$ ou 2.

Solução: Seja $d = (a + b, a - b)$. Logo $a + b = k_1 d$ e $a - b = k_2 d$ e, portanto

$$(k_1 + k_2)d = 2a \quad \text{e} \quad (k_1 - k_2)d = 2b.$$

Sabemos que $(2a, 2b) = 2(a, b) = 2$. Mas $(2a, 2b) = ((k_1 + k_2)d, (k_1 - k_2)d) = d(k_1 + k_2, k_1 - k_2) = 2$. Considerando $(k_1 + k_2, k_1 - k_2) = k$ temos $dk = 2$ o

que ocorre se, e somente se, $d = 1$ e $k = 2$ ou $d = 2$ e $k = 1$. Portanto $d = 1$ ou $d = 2$. □

Problema 1.14 Mostrar que se $a^n - 1$ for primo, $n > 1$ e $a > 1$ então $a = 2$ e n é primo.

Solução: Como $a^n - 1 = (a-1)(a^{n-1} + a^{n-2} + \cdots + a + 1)$, e o fator da direita é maior do $1 (a > 1)$ concluimos que $a - 1$ deve ser igual a 1 uma vez que $a^n - 1$ é primo. Portanto a deve ser igual a 2.

Se n não for primo então $n = rs, r > 1$ e $s > 1$. Disto concluimos que

$$2^{rs} - 1 = (2^r - 1)(2^{r(s-1)} + 2^{r(s-2)} + \cdots + 2^r + 1)$$

o que contradiz o fato de $2^{rs} - 1$ ser primo, o que implica que n deve ser primo.

1.10 Problemas Propostos

1. Encontrar, usando o algoritmo de Euclides, o máximo divisor comum dos seguintes pares de números:

(a) 542 e 234
(b) 9652 e 252
(c) 24573 e 1387
(d) 4276 e 1234
(e) 48762 e 176
(f) 42516 e 97421
(g) 8374, 24517
(h) 35262 e 12753

2. Achar o mínimo múltiplo comum dos seguintes pares de números:

(a) 44 e 32
(b) 234 e 12
(c) 35 e 24
(d) 142 e 742
(e) 17 e 141
(f) 42 e 52
(g) 501 e 2141
(h) 144 e 64

3. Encontrar uma seqüência de pelo menos 30 inteiros consecutivos e compostos.

4. Mostrar, por indução, que

(a) $1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$
(b) $1 + 3 + 5 + \cdots + (2n-1) = n^2$
(c) $1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + \cdots + n(n+1) = \frac{n(n+1)(n+2)}{3}$
(d) $n! > 2^n$, $\forall n \geq 4$
(e) $n^2 > 2n + 1$, $\forall n \geq 3$
(f) $9 | (10^{n+1} - 9n - 10)$, $\forall n \geq 1$

5. Provar que o produto de 3 inteiros consecutivos é divisível por 6.

6. Provar que para todo $n \in \mathbb{N}$, $3^{2n+1} + 2^{n+2}$ é múltiplo de 7 e que $3^{2n+2} + 2^{6n+1}$ é múltiplo de 11.

7. Encontrar inteiros x e y tais que

(a) $93x + 81y = 3$
(b) $43x + 128y = 1$

8. Mostrar que se a e b são inteiros positivos com $(a, b) = [a, b]$, então $a = b$.

9. Mostrar que $n^5 - n$ é divisível por 30 para todo inteiro n.

10. Mostrar que a equação $x^3 + 7x + 17 = 0$ não possui nenhuma solução inteira.

11. Mostrar que para nenhum $n \in \mathbb{N}, 2^n + 1$ é um cubo.

12. Pode o número $A = 111 \ldots 1$ formado por trezentos $1's$ ser um quadrado?

13. Sejam $F_1 = 1, F_2 = 1$ e $F_n = F_{n-1} + F_{n-2}, n \geq 3$ (F_n é chamado n-ésimo número de Fibonacci). Mostrar que

(a) $F_1 + F_3 + F_5 + \cdots + F_{2n-1} = F_{2n}$
(b) $F_2 + F_4 + F_6 + \cdots + F_{2n} = F_{2n+1} - 1$
(c) $F_1 + F_2 + F_3 + \cdots + F_n = F_{n+2} - 1$
(d) $F_1F_2 + F_2F_3 + F_3F_4 + \cdots + F_{2n}F_{2n+1} = F_{2n+1}^2 - 1$

14. Mostrar que para os números de Fibonacci, definidos no problema anterior, satisfazem

(a) $(F_n, F_{n+1}) = 1$
(b) $(F_n, F_{n+3}) = 1$ ou 2.

15. Mostrar que além de $2 = 1^3 + 1$ nenhum número da forma $n^3 + 1$ é primo.

16. Utilizando a sequência $R_n = n! + 1, n \geq 1$, fornecer uma outra demonstração para a infinitude dos primos.

17. Mostrar que todo inteiro maior do que 11 é a soma de dois inteiros compostos.

18. Mostrar que 3 é o único primo p tal que $p, p+2$ e $p+4$ são todos primos.

19. Achar a soma de todos os números formados pelas permutações dos dígitos 1,2,3,4 e 5, isto é: $12345 + \cdots + 54321$.

20. Provar que não existe $n \in \mathbb{N}$ tal que $7 | (4n^2 - 3)$

21. Sabendo que o resto da divisão de um inteiro b por 7 é 5, calcular o resto da divisão por 7 dos seguintes números:

(a) $-b$
(b) $2b$
(c) $3b + 7$
(d) $10b + 1$
(e) $b^2 + b + 1$

22. Seja $U_n = 111\ldots1$ um número formado por n 1's. Provar que U_n primo implica n primo.

23. Mostrar que se para algum n, $m|(35n+26)$, $m|(7n+3)$ e $m > 1$, então $m = 11$.

24. Sendo $\frac{1}{a} + \frac{1}{b}$ um inteiro, onde a e b são inteiros positivos, mostrar que $a = b$. Mostrar, também, que $a = 1$ ou 2.

25. Mostrar que se $(a, b) = 1$, então $(2a + b, a + 2b) = 1$ ou 3.

26. Mostrar que, sendo n um inteiro, o número $n(n+1)(n+2)(n+3)+1$ é um quadrado perfeito.

27. Determinar todos o números de 3 algarismos divisíveis por 8, 11 e 12.

28. Encontrar todos os inteiros positivos n para os quais $(n+1)|(n^2+1)$.

29. Dados a e b inteiros com $b \neq 0$, mostrar que existem inteiros q e r satisfazendo $a = qb \pm r$, $0 \leq r \leq b/2$.

30. Mostrar que se a e b são inteiros, $(a,3) = (b,3) = 1$, então $a^2 + b^2$ não é um quadrado perfeito.

31. Mostrar que para $n > 1$ os números $n^4 + 4$ e $n^4 + n^2 + 1$ são, ambos, compostos.

32. Demonstrar os ítens (a), (b) e (c) do problema 13 sem fazer uso de indução.

33. Mostrar que $(a, bc) = 1$, se, e somente se, $(a, b) = (a, c) = 1$.

34. Mostrar que se $b|c$ então $(a + c, b) = (a, b)$

35. Mostrar que se $(a, c) = 1$ então $(a, bc) = (a, b)$.

36. Mostrar que $(a, b, c) = ((a, b), c)$.

37. Dizer qual é o maior inteiro que pode ser somado ao dividendo sem alterar o quociente quando se divide 431 por 37.

38. Para cada par de inteiros "a"e "b"dado abaixo encontrar o quociente q e o resto r satisfazendo o algoritmo da divisão de Euclides.

(i) $a = 59$; $b = 6$
(ii) $a = -71$; $b = 5$
(iii) $a = -48$; $b = -7$
(iv) $a = 67$; $b = -13$

39. Mostrar que se n e m são inteiros ímpares, então $8|(n^4 + m^4 - 2)$.

40. Encontrar o menor inteiro positivo da forma $36x + 54y$ onde x e y são inteiros.

41. Utilizando o processo descrito no Teorema 1.17 expressar o número 274 nas bases 2,5,7 e 9.

42. Transformar para a base 10 os seguintes números
(a) $(2351)_7$ (b) $(1001110)_2$ (c) $(7706)_8$ (d) $(11122)_4$

43. Mostrar que se $2^n + 1$ é um primo ímpar, então n é uma potência de 2.

44. Provar que se $d = (a, b)$, então d é o número de inteiros na seqüência $a, 2a, 3a, \ldots, ba$ que são divisíveis por b.

Capítulo 2

Congruência

2.1 Congruência

Grande parte dos resultados deste capítulo foi introduzida por Gauss (1777-1855) em um trabalho publicado em 1801 (*Disquisitiones Arithmeticae*) quando tinha apenas 24 anos. Várias idéias de grande importância, que serviram de base para o desenvolvimento da teoria de números, aparecem neste trabalho. Até mesmo a notação, lá introduzida, é a que utilizamos hoje.

Definição 2.1 Se a e b são inteiros dizemos que a é *congruente* a b módulo m $(m > 0)$ se $m|(a-b)$. Denotamos isto por $a \equiv b \pmod{m}$. Se $m \nmid (a-b)$ dizemos que a é *incongruente* a b módulo m e denotamos $a \not\equiv b \pmod{m}$.

Exemplo 2.1 $11 \equiv 3 \pmod{2}$ pois $2|(11-3)$. Como $5 \nmid 6$ e $6=17-11$ temos que $17 \not\equiv 11 \pmod{5}$.

Proposição 2.1 *Se* a *e* b *são inteiros, temos que* $a \equiv b \pmod{m}$ *se, e somente se, existir um inteiro* k *tal que* $a = b + km$.

Demonstração: Se $a \equiv b \pmod{m}$, então $m|(a-b)$ o que implica na existência de um inteiro k tal que $a - b = km$, isto é, $a = b + km$. A recíproca é trivial pois da existência de um k satisfazendo $a = b + km$, temos $km = a - b$, ou seja, que $m|(a-b)$ isto é, $a \equiv b \pmod{m}$. □

Proposição 2.2 *Se* a, b, m *e* d *são inteiros,* $m > 0$*, as seguintes sentenças são verdadeiras:*

1. $a \equiv a \pmod{m}$
2. Se $a \equiv b \pmod{m}$, então $b \equiv a \pmod{m}$
3. Se $a \equiv b \pmod{m}$ e $b \equiv d \pmod{m}$, então $a \equiv d \pmod{m}$.

Demonstração: (1) Como $m|0$, então $m|(a-a)$, o que implica $a \equiv a \pmod{m}$. (2) Se $a \equiv b \pmod{m}$, então $a = b + k_1 m$ para algum inteiro k_1. Logo $b = a - k_1 m$, o que implica, pela Proposição 2.1, $b \equiv a \pmod{m}$. (3) Se $a \equiv b \pmod{m}$ e $b \equiv d \pmod{m}$, então existem inteiros k_1 e k_2 tais que $a - b = k_1 m$ e $b - d = k_2 m$. Somando-se, membro a membro, estas últimas equações, obtemos $a - d = (k_1 + k_2)m$, o que implica $a \equiv d \pmod{m}$. □

Esta proposição nos diz que a relação de congruência, definida no conjunto dos inteiros, é uma relação de equivalência, pois acabamos de provar que ela é reflexiva, simétrica e transitiva.

Teorema 2.1 *Se* a, b, c *e* m *são inteiros tais que* $a \equiv b \pmod{m}$*, então*

1. $a + c \equiv b + c \pmod{m}$
2. $a - c \equiv b - c \pmod{m}$
3. $ac \equiv bc \pmod{m}$

Demonstração: (1) Como $a \equiv b \pmod{m}$, temos que $a - b = km$ e, portanto, como $a - b = (a + c) - (b + c)$ temos $a + c \equiv b + c \pmod{m}$. (2) Como $(a - c) - (b - c) = a - b$ e, por hipótese, $a - b = km$ temos que $a - c \equiv b - c \pmod{m}$. (3) Como $a - b = km$ então $ac - bc = ckm$ o que implica $m|(ac - bc)$ e, portanto, $ac \equiv bc \pmod{m}$. □

Teorema 2.2 *Se* a, b, c, d *e* m *são inteiros tais que* $a \equiv b \pmod{m}$ *e* $c \equiv d \pmod{m}$*, então*

1. $a + c \equiv b + d \pmod{m}$
2. $a - c \equiv b - d \pmod{m}$
3. $ac \equiv bd \pmod{m}$

Demonstração: (1) De $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$ temos $a - b = km$ e $c - d = k_1 m$. Somando-se membro a membro obtemos $(a + c) - (b + d) = (k + k_1)m$ e isto implica $a + c \equiv b + d \pmod{m}$. (2) Basta subtrair membro a membro $a - b = km$ e $c - d = k_1 m$ obtendo $(a-b)-(c-d) = (a-c)-(b-d) = (k - k_1)m$ o que implica $a - c \equiv b - d \pmod{m}$. (3) Multiplicamos ambos os lados de $a - b = km$ por c e ambos os lados de $c - d = k_1 m$ por b, obtendo $ac - bc = ckm$ e $bc - bd = bk_1 m$. Basta, agora, somarmos membro a membro estas últimas igualdades obtendo $ac - bc + bc - bd = ac - bd = (ck + bk_1)m$ o que implica $ac \equiv bd \pmod{m}$. □

Teorema 2.3 *Se* a, b, c *e* m *são inteiros e* $ac \equiv bc \pmod{m}$, *então* $a \equiv b \pmod{m/d}$ *onde* $d = (c, m)$.

Demonstração: De $ac \equiv bc \pmod{m}$ temos $ac - bc = c(a-b) = km$. Se dividirmos os dois membros por d, teremos $(c/d)(a-b) = k(m/d)$. Logo $(m/d)|(c/d)(a-b)$ e, como $(m/d, c/d) = 1$, pelo Teorema 1.6, $(m/d)|(a-b)$ o que implica $a \equiv b \pmod{m/d}$. □

Definição 2.2 Se h e k são dois inteiros com $h \equiv k \pmod{m}$, dizemos que k é um *resíduo* de h módulo m.

Definição 2.3 O conjunto dos inteiros $\{r_1, r_2, \ldots, r_s\}$ é um *sistema completo de resíduos* módulo m se
(1) $r_i \not\equiv r_j \pmod{m}$ para $i \neq j$
(2) para todo inteiro n existe um r_i tal que $n \equiv r_i \pmod{m}$.

Exemplo 2.2 $\{0, 1, 2, \ldots, m-1\}$ é um sistema completo de resíduos módulo m.

Exemplo 2.3 Para m ímpar o conjunto abaixo é um sistema completo de resíduos módulo m.

$$\left\{-\frac{m-1}{2}, -\frac{m-3}{2}, \ldots, -1, 0, 1, \ldots, \frac{m-3}{2}, \frac{m-1}{2}\right\}$$

Teorema 2.4 *Se* k *inteiros* $r_1, r_2, \ldots, r_k$ *formam um sistema completo de resíduos módulo* m *então* $k = m$.

Demonstração: Primeiramente demonstramos que os inteiros $t_0, t_1, \ldots, t_{m-1}$, com $t_i = i$ formam, de fato, um sistema completo de resíduos módulo m. Pelo Teorema 1.2 sabemos que, para cada n, existe um único par de inteiros q e s, tal que $n = mq + s$, $0 \leq s < m$. Logo $n \equiv s \pmod{m}$, sendo s um dos t_i. Como $|t_i - t_j| \leq m - 1$, temos que $t_i \not\equiv t_j \pmod{m}$ para $i \neq j$. Portanto, o conjunto $\{t_0, t_1, \ldots, t_{m-1}\}$ é um sistema completo de resíduos módulo m. Disto concluímos que cada r_i é congruente a exatamente um dos t_i, o que nos garante $k \leq m$. Como o conjunto $\{r_1, r_2, \ldots, r_k\}$ forma, por hipótese, um sistema completo de resíduos módulo m, cada t_i é congruente a exatamente um dos r_i e portanto $m \leq k$. Desta forma $k = m$. □

Teorema 2.5 *Se* $r_1, r_2, \ldots, r_m$ *é um sistema completo de resíduos módulo* m *e* a *e* b *são inteiros com* $(a, m) = 1$, *então*

$$ar_1 + b, ar_2 + b, \ldots, ar_m + b$$

também é um sistema completo de resíduos módulo m.

Demonstração: Considerando-se o resultado do teorema anterior, será suficiente mostrar que quaisquer dois inteiros do conjunto $ar_1+b, ar_2+b, \ldots, ar_m+b$, são incongruentes módulo m. Para isto vamos supor que $ar_i + b \equiv ar_j + b \pmod{m}$. Logo, pelo Teorema 2.1, temos $ar_i \equiv ar_j \pmod{m}$. Mas, como $(a, m) = 1$, o Teorema 2.3 nos diz que $r_i \equiv r_j \pmod{m}$. O fato de $r_i \equiv r_j \pmod{m}$ implica $i = j$, uma vez que, $r_1, r_2, \ldots, r_m$ formam um sistema completo de resíduos módulo m, o que completa a demonstração. □

Proposição 2.3 *Se* a, b, k *e* m *são inteiros com* $k > 0$ *e* $a \equiv b \pmod{m}$, *então* $a^k \equiv b^k \pmod{m}$.

Demonstração: Isto segue, imediatamente, da identidade:

$$a^k - b^k = (a-b)(a^{k-1} + a^{k-2}b + a^{k-3}b^2 + \cdots + ab^{k-2} + b^{k-1}).$$

Teorema 2.6 *Se* $a \equiv b \pmod{m_1}, a \equiv b \pmod{m_2}, \ldots, a \equiv b \pmod{m_k}$ *onde* $a, b, m_1, m_2, \ldots, m_k$ *são inteiros com* m_i *positivos,* $i = 1, 2, \ldots, k$, *então*

$$a \equiv b \pmod{[m_1, m_2, \ldots, m_k]}$$

onde $[m_1, m_2, \ldots, m_k]$ *é o mínimo múltiplo comum de* $m_1, m_2, \ldots, m_k$.

Demonstração: Seja p_n o maior primo que aparece nas fatorações de $m_1, m_2, \ldots, m_k$. Cada m_i, $i = 1, 2, \ldots, k$ pode, então, ser expresso como

$$m_i = p_1^{\alpha_{1i}} \cdot p_2^{\alpha_{2i}} \cdots p_n^{\alpha_{ni}},$$

(alguns α_{ji} podem ser nulos).

Como $m_i|(a-b), i = 1, 2, \ldots, k$ temos que $p_j^{\alpha_{ji}}|(a-b), i = 1, 2, \ldots, k$, $j = 1, 2, \ldots, n$. Logo, se tomarmos $\alpha_j = \max_{1 \leq i \leq k}\{\alpha_{ji}\}$ teremos que

$$p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_n^{\alpha_n}|(a-b).$$

Mas,

$$p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_n^{\alpha_n} = [m_1, m_2, \ldots, m_k]$$

o que implica $a \equiv b \pmod{[m_1, m_2, \ldots, m_k]}$. □

2.2 Congruência Linear

Chamamos de *congruência linear* em uma variável a uma congruência da forma $ax \equiv b \pmod{m}$ onde x é uma incógnita.

É fácil de se verificar que se x_0 é uma solução, i.e., $ax_0 \equiv b \pmod m$ e $x_1 \equiv x_0 \pmod m$ então x_1 também é solução. Isto é óbvio pois se $x_1 \equiv x_0 \pmod m$ então $ax_1 \equiv ax_0 \equiv b \pmod m$.

O que acabamos de verificar é que se um membro de uma classe de equivalência é solução então todo membro desta classe é solução. Destas observações surge uma questão natural: no caso de existir alguma solução, quantas soluções incongruentes existem?

Antes de respondermos a esta importante questão, necessitamos provar um teorema que nos dá informações sobre a existência de soluções para uma equação diofantina linear.

Uma equação da forma $ax + by = c$, onde a, b e c são inteiros é chamada *equação diofantina linear*. (o nome vem do matemático grego Diofanto).

Teorema 2.7 *Sejam a e b inteiros positivos e $d = (a, b)$. Se $d \nmid c$ então a equação $ax + by = c$ não possui nenhuma solução inteira. Se $d|c$ ela possui infinitas soluções e se $x = x_0$ e $y = y_0$ é uma solução particular, então todas as soluções são dadas por*

$$\begin{aligned} x &= x_0 + (b/d)k \\ y &= y_0 - (a/d)k \end{aligned}$$

onde k é um inteiro.

Demonstração: Se $d \nmid c$, então a equação $ax + by = c$, não possui solução pois, como $d|a$ e $d|b$, d deveria dividir c, o qual é uma combinação linear de a e b. Suponhamos, pois, que $d|c$. Pelo Teorema 1.3 existem inteiros n_0 e m_0, tais que

$$an_0 + bm_0 = d. \tag{2.1}$$

Como $d|c$, existe um inteiro k tal que $c = kd$. Se multiplicarmos, ambos os membros de (2.1) por k, teremos $a(n_0k) + b(m_0k) = kd = c$. Isto nos diz que o par (x_0, y_0) com $x_0 = n_0k$ e $y_0 = m_0k$ é uma solução de $ax + by = c$. É fácil a verificação de que os pares da forma

$$\begin{aligned} x &= x_0 + (b/d)k \\ y &= y_0 - (a/d)k \end{aligned}$$

são soluções, uma vez que

$$\begin{aligned} ax + by &= a(x_0 + (b/d)k) + b(y_0 - (a/d)k) \\ &= ax_0 + \frac{ab}{d}k + by_0 - \frac{ab}{d}k \end{aligned}$$

$$= ax_0 + by_0 = c.$$

O que acabamos de mostrar é que, conhecida uma solução particular (x_0, y_0) podemos, a partir dela, gerar infinitas soluções. Precisamos, agora, mostrar que toda solução da equação $ax + by = c$ é da forma $x = x_0 + (b/d)k$, $y = y_0 - (a/d)k$. Vamos supor que (x, y) seja uma solução, i.e., $ax + by = c$. Mas, como $ax_0 + by_0 = c$, obtemos, subtraindo membro a membro, que

$$ax + by - ax_0 - by_0 = a(x - x_0) + b(y - y_0) = 0,$$

o que implica $a(x - x_0) = b(y_0 - y)$. Como $d = (a, b)$ temos, pelo corolário da Proposição 1.4,

$$\left(\frac{a}{d}, \frac{b}{d}\right) = 1.$$

Portanto, dividindo-se os dois membros da última igualdade por d, teremos

$$\frac{a}{d}(x - x_0) = \frac{b}{d}(y_0 - y). \tag{2.2}$$

Logo, pelo Teorema 1.6, $(b/d)|(x - x_0)$ e portanto existe um inteiro k satisfazendo $x - x_0 = k(b/d)$, ou seja $x = x_0 + (b/d)k$. Substituindo-se este valor de x na equação (2.2) temos $y = y_0 - (a/d)k$, o que conclui a demonstração. □

Com este teorema à mão podemos, agora, dizer quantas são as soluções incongruentes (caso exista alguma) que a congruência linear $ax \equiv b \pmod m$ possui.

Teorema 2.8 *Sejam a, b e m inteiros tais que $m > 0$ e $(a, m) = d$. No caso em que $d \nmid b$ a congruência $ax \equiv b \pmod m$ não possui nenhuma solução e quando $d|b$, possui exatamente d soluções incongruentes módulo m.*

Demonstração: Pela Proposição 2.1 sabemos que o inteiro x é solução de $ax \equiv b \pmod m$ se, e somente se, existe um inteiro y tal que $ax = b + my$, ou, o que é equivalente, $ax - my = b$. Do teorema anterior sabemos que esta equação não possui nenhuma solução caso $d \nmid b$, e que se $d|b$ ela possui infinitas soluções dadas por $x = x_0 - (m/d)k$ e $y = y_0 - (a/d)k$ onde (x_0, y_0) é uma solução particular de $ax - my = b$. Logo a congruência $ax \equiv b \pmod m$ possui infinitas soluções dadas por $x = x_0 - \left(\frac{m}{d}\right)k$. Como estamos interessados em saber o número de soluções incongruentes, vamos tentar descobrir sob que condições $x_1 = x_0 - (m/d)k_1$ e $x_2 = x_0 - (m/d)k_2$ são congruentes módulo m. Se x_1 e x_2 são congruentes então $x_0 - (m/d)k_1 \equiv x_0 - (m/d)k_2 \pmod m$. Isto implica $(m/d)k_1 \equiv (m/d)k_2 \pmod m$, e como $(m/d)|m$, temos $(m/d, m) = m/d$, o que nos permite o cancelamento de m/d resultando, pelo Teorema 2.3,

$k_1 \equiv k_2 (\text{mod } d)$. Observe que m foi substituído por $d = m/(m/d)$. Isto nos mostra que soluções incongruentes serão obtidas ao tomarmos $x = x_0 - (m/d)k$, onde k percorre um sistema completo de resíduos módulo d, o que conclui a demonstração. □

Definição 2.4 Dizemos que uma solução x_0 de $ax \equiv b(\text{mod } m)$ é única módulo m quando qualquer outra solução x_1 for congruente a x_0 módulo m.

Definição 2.5 Uma solução $\overline{a}$ de $ax \equiv 1(\text{mod } m)$ é chamada de um *inverso* de a módulo m.

Segue, agora, do Teorema 2.8 que se $(a, m) = 1$ então a possui um único inverso módulo m. A proposição seguinte nos diz quando um inteiro a é o seu próprio inverso módulo p, onde p é um número primo.

Proposição 2.4 *Seja p um número primo. O inteiro positivo a é o seu próprio inverso módulo p se, e somente se, $a \equiv 1(\text{mod } p)$ ou $a \equiv -1(\text{mod } p)$.*

Demonstração: Se a é o seu próprio inverso, então $a^2 \equiv 1(\text{mod } p)$, o que significa que $p|(a^2-1)$. Mas se $p|(a-1)(a+1)$, sendo p primo, $p|(a-1)$ ou $p|(a+1)$, o que implica $a \equiv 1(\text{mod } p)$ ou $a \equiv -1(\text{mod } p)$. A recíproca é imediata pois, se $a \equiv 1(\text{mod } p)$ ou $a \equiv -1(\text{mod } p)$, então $p|(a-1)$ ou $p|(a+1)$. Portanto $p|(a-1)(a+1)$ o que significa $a^2 \equiv 1(\text{mod } p)$, o que conclui a demonstração. □

2.3 Os Teoremas de Euler, Fermat e Wilson

Antes de demonstrarmos o Teorema de Wilson, que diz que para p primo $(p-1)! \equiv -1(\text{mod } p)$, fornecemos um exemplo, tomando $p = 13$, com a finalidade de apresentarmos a idéia utilizada na demonstração.

Dentre os números 1,2,3,...,12 somente os números 1 e 12 são os seus próprios inversos módulo 13. Isto segue da Proposição 2.4, pois $1 \equiv 1(\text{mod } 13)$ e $12 \equiv -1(\text{mod } 13)$ e nenhum dos números $2, 3, \ldots, 11$ é congruente a 1 ou -1 módulo 13. Mas, como os números $2, 3, 4, \ldots, 11$ são todos relativamente primos com 13, cada um deles possui, pelo Teorema 2.8, um único inverso módulo 13. Eles podem, portanto, ser agrupados em 5 pares $(5 = (13-3)/2)$ que são os seguintes:

$$\begin{aligned}
2 \times 7 &\equiv 1(\text{mod } 13)\\
3 \times 9 &\equiv 1(\text{mod } 13)\\
4 \times 10 &\equiv 1(\text{mod } 13)\\
5 \times 8 &\equiv 1(\text{mod } 13)\\
6 \times 11 &\equiv 1(\text{mod } 13)
\end{aligned}$$

Pelo Teorema 2.2(3) podemos multiplicar estas congruências, membro a membro, obtendo

$$2 \times 3 \times 4 \times 5 \times 6 \times 7 \times 8 \times 9 \times 10 \times 11 \equiv 1(\text{mod } 13)$$

Se multiplicarmos os dois lados por 12 teremos

$$2 \times 3 \times 4 \ldots 11 \times 12 \equiv 12(\text{mod } 13)$$

e, portanto, como $12 \equiv -1(\text{mod } 13)$ temos, finalmente, $(13-1)! \equiv -1(\text{mod } 13)$.

Teorema 2.9 (Teorema de Wilson) *Se p é primo, então $(p-1)! \equiv -1(\text{mod } p)$.*

Primeira Demonstração: Como $(2-1)! \equiv 1 \equiv -1(\text{mod } 2)$ o resultado é válido para $p = 2$. Pelo Teorema 2.8, a congruência $ax \equiv 1(\text{mod } p)$ tem uma única solução para todo a no conjunto $\{1, 2, 3, \ldots, p-1\}$ e como, destes elementos, somente 1 e $p-1$ são seus próprios inversos módulo p, podemos agrupar os números $2, 3, 4, \ldots, p-2$ em $(p-3)/2$ pares cujo produto seja congruente a 1 módulo p. Se multiplicarmos estas congruências, membro a membro, teremos, pelo Teorema 2.2 (3) $2 \times 3 \times 4 \times 5 \times \ldots (p-2) \equiv 1(\text{mod } p)$. Multiplicando-se ambos os lados desta congruência por $p-1$ teremos

$$2 \times 3 \times 4 \times \ldots (p-2)(p-1) \equiv (p-1)(\text{mod } p)$$

isto é $(p-1)! \equiv -1(\text{mod } p)$ uma vez que $p-1 \equiv -1(\text{mod } p)$. □

Segunda Demonstração: Esta segunda demonstração foi apresentada por Stern e ilustra o uso de análise em Teoria dos Números. A primeira segue, essencialmente, Gauss.

Consideramos a expansão de Maclaurin da função

$$\ln\left(\frac{1}{1-x}\right),$$

isto é,

$$\ln\frac{1}{1-x} = x + \frac{x^2}{2} + \frac{x^3}{3} + \cdots; \qquad -1 \leq x < 1.$$

Logo

$$e^{x+\frac{x^2}{2}+\frac{x^3}{3}+\cdots} = \frac{1}{1-x} = 1 + x + x^2 + x^3 + \cdots \tag{2.3}$$

O lado esquerdo desta igualdade pode ser escrito como

$$e^x e^{\frac{x^2}{2}} e^{\frac{x^3}{3}} \cdots = \left(1 + \frac{x}{1!} + \frac{x^2}{2!} + \cdots\right).$$

$$\left(1+\frac{x^2/2}{1!}+\frac{(x^2/2)^2}{2!}+\cdots\right)\cdots$$
$$\left(1+\frac{x^p/p}{1!}+\frac{(x^p/p)^2}{2!}+\cdots\right)\cdots$$
$$=1+\frac{x}{1!}+x^2\left(\frac{1}{2!}+\frac{1}{2}\right)+x^3\left(\frac{1}{3!}+\frac{1}{1!}\,\frac{1/2}{1!}+\frac{1/3}{1!}\right)+\cdots$$
$$+x^p\left(\frac{1}{p!}+\frac{1}{(p-2)!}\,\frac{1/2}{1!}+\cdots+\frac{1/p}{1!}\right)+\cdots$$

Por (2.3) sabemos que o coeficiente de x^p é igual a 1 o qual, pela expressão acima é da forma $\frac{1}{p!}+\frac{r}{s}+\frac{1}{p}$ onde r/s é a soma de um número finito de racionais que não possuem o fator p no denominador. Logo se $(r,s)=1, p\nmid s$.

Sendo $\frac{1}{p!}+\frac{r}{s}+\frac{1}{p}=1$ temos que

$$1-\frac{r}{s}=\frac{1}{p!}+\frac{1}{p}=\frac{(1+(p-1)!)}{p!}$$

e, portanto,

$$(s-r)\,(p-1)!=\frac{s(1+(p-1)!)}{p}.$$

Como $(s-r)\,(p-1)!$ é um inteiro e $p\nmid s$, então $p|(1+(p-1)!)$. □

O teorema seguinte nos diz que se um número satisfaz a relação do teorema de Wilson, ele deve ser primo.

Teorema 2.10 *Se n é um inteiro tal que $(n-1)!\equiv -1(\text{mod } n)$, então n é primo.*

Demonstração: A prova é por contradição. Vamos supor que $(n-1)!\equiv -1(\text{mod } n)$, isto é, $n|((n-1)!+1)$ e que n não seja primo, ou seja, $n=rs, 1<r<n$ e $1<s<n$. Nestas condições $r|(n-1)!$ e, sendo r um divisor de $n, r|(n-1)!+1$ e, portanto, r deve dividir a diferença $(n-1)!+1-(n-1)!=1$, o que é absurdo, uma vez que $r>1$. Logo, um n satisfazendo $(n-1)!\equiv -1(\text{mod } n)$ deve ser primo. □

O próximo teorema nos diz que se p é primo e $p\nmid a$, então $p|(a^{p-1}-1)$. Vamos primeiramente provar isto num caso particular com a finalidade de ilustrar a idéia usada na demonstração.

Sejam $p=11$ e $a=5$. Logo temos:

$$\begin{aligned}
1\times 5 &\equiv 5(\text{mod } 11)\\
2\times 5 &\equiv 10(\text{mod } 11)\\
3\times 5 &\equiv 4(\text{mod } 11)\\
4\times 5 &\equiv 9(\text{mod } 11)\\
5\times 5 &\equiv 3(\text{mod } 11)\\
6\times 5 &\equiv 8(\text{mod } 11)\\
7\times 5 &\equiv 2(\text{mod } 11)\\
8\times 5 &\equiv 7(\text{mod } 11)\\
9\times 5 &\equiv 1(\text{mod } 11)\\
10\times 5 &\equiv 6(\text{mod } 11)
\end{aligned}$$

Observe que 11 não divide nenhum dos produtos $j\times 5, 1\leq j\leq 10$ que estão na coluna da esquerda nas congruências acima. Observe, também, que todos eles são incongruentes módulo 11, pois se $5j\equiv 5k(\text{mod } 11)$, devemos ter $j\equiv k(\text{mod } 11)$ com $1\leq j\leq 10$ e $1\leq k\leq 10$, e, portanto, $j=k$. Logo, como nenhum é congruente a zero módulo 11 e todos são incongruentes módulo 11, eles devem ser congruentes a diferentes números dentre $1,2,3,\ldots,10$. Observe que todos estes números aparecem, sem repetições, na coluna da direita nas congruências acima. Agora podemos multiplicar, membro a membro, estas congruências para obter

$$(1\times 5)(2\times 5)\cdots(10\times 5)\equiv 5\times 10\times 4\times 9\times 3\times 8\times 2\times 7\times 1\times 6(\text{mod } 11)$$

e, portanto, $5^{10}10!\equiv 10!(\text{mod } 11)$. Mas, como $(10!,11)=1$ temos, pelo Teorema 2.3, que

$$5^{10}\equiv 1(\text{mod } 11),$$

o que mostra a validade do teorema neste caso particular em que $a=5$ e $p=11$. Com este exemplo em mente será fácil provar o teorema.

Teorema 2.11 (Pequeno Teorema de Fermat) *Seja p primo. Se $p\nmid a$ então $a^{p-1}\equiv 1(\text{mod } p)$.*

Demonstração: Sabemos que o conjunto formado pelos p números $0,1,2,\ldots,p-1$ constitui um sistema completo de resíduos módulo p. Isto significa que qualquer conjunto contendo no máximo p elementos incongruentes módulo p pode ser colocado em correspondência biunívoca com um subconjunto de $\{0,1,2,\ldots,p-1\}$. Vamos, agora, considerar os números $a,2a,3a,\ldots,(p-1)a$. Como $(a,p)=1$, nenhum destes números $ia, 1\leq i\leq p-1$ é divisível por p, ou seja, nenhum é congruente a zero módulo p.

Quaisquer dois deles são incongruentes módulo p, pois $aj \equiv ak \pmod p$ implica $j \equiv k \pmod p$ e isto só é possível se $j = k$, uma vez que ambos j e k são positivos e menores do que p. Temos, portanto, um conjunto de $p-1$ elementos incongruentes módulo p e não-divisíveis por p. Logo, cada um deles é congruente a exatamente um dentre os elementos $1, 2, 3, \ldots, p-1$. Se multiplicarmos estas congruências, membro a membro, teremos:

$$a(2a)(3a)\cdots(p-1)a \equiv 1.2.3\cdots(p-1) \pmod p$$

ou seja $a^{p-1}(p-1)! \equiv (p-1)! \pmod p$. Mas, como $((p-1)!, p) = 1$, podemos cancelar o fator $(p-1)!$ em ambos os lados, obtendo

$$a^{p-1} \equiv 1 \pmod p,$$

o que conclui a demonstração. □

Corolário 2.1 *Se p é um primo e a é um inteiro positivo, então $a^p \equiv a \pmod p$.*

Demonstração: Temos que analisar dois casos, se $p|a$ e se $p\nmid a$. Se $p|a$, então $p|(a(a^{p-1}-1))$ e, portanto $a^p \equiv a \pmod p$. Se $p\nmid a$, pelo Teorema 2.11 $p|(a^{p-1}-1)$ e, portanto, $p|(a^p - a)$. Logo, em ambos os casos, $a^p \equiv a \pmod p$. □

Definição 2.6 Se n é um inteiro positivo, a *função ϕ de Euler*, denotada por $\phi(n)$, é definida como sendo o número de inteiros positivos menores do que ou iguais a n que são relativamente primos com n.

Definição 2.7 Um *sistema reduzido de resíduos* módulo m é um conjunto de $\phi(m)$ inteiros $r_1, r_2, \ldots, r_{\phi(m)}$, tais que cada elemento do conjunto é relativamente primo com m, e se $i \neq j$, então $r_i \not\equiv r_j \pmod m$.

Exemplo 2.4 O conjunto $\{0, 1, 2, 3, 4, 5, 6, 7\}$ é um sistema completo de resíduos módulo 8, portanto $\{1, 3, 5, 7\}$ é um sistema reduzido de resíduos módulo 8. A fim de se obter um sistema reduzido de resíduos de um sistema completo módulo m, basta retirar os elementos do sistema completo que não são relativamente primos com m.

Teorema 2.12 *Seja a um inteiro positivo tal que $(a, m) = 1$. Se $r_1, r_2, \ldots, r_{\phi(m)}$ é um sistema reduzido de resíduos módulo m, então $ar_1, ar_2, \ldots, ar_{\phi(m)}$ é, também, um sistema reduzido de resíduos módulo m.*

Demonstração: Como na seqüência $ar_1, ar_2, \ldots, ar_{\phi(m)}$ temos $\phi(m)$ elementos, devemos mostrar que todos eles são relativamente primos com m e, dois a dois, incongruentes módulo m. Como $(a, m) = 1$ e $(r_i, m) = 1$, temos (veja Problema 1.33 no final do cap. 1), $(ar_i, m) = 1$. Logo, nos resta mostrar que $ar_i \not\equiv ar_j \pmod m$ se $i \neq j$. Mas, como $(a, m) = 1$, de $ar_i \equiv ar_j \pmod m$ temos $r_i \equiv r_j \pmod m$, o que implica $i = j$, uma vez que $r_1, r_2, \ldots, r_{\phi(m)}$, é um sistema reduzido de resíduos módulo m, o que conclui a demonstração. □ Vamos, agora, mostrar a validade do Teorema de Euler num caso especial para ilustrar a idéia que usaremos na demonstração. Sejam $m = 8$ e $a = 5$. Sabemos que o conjunto $\{1, 3, 5, 7\}$ é um sistema reduzido de resíduos módulo 8. Consideremos o conjunto formado por $5\times1, 5\times3, 5\times5$ e 5×7. Pelo Teorema 2.12 este conjunto também constitui um sistema reduzido de resíduos módulo 8. Isto significa que cada um dos elementos 5×1, 5×3, 5×5 e 5×7 é congruente módulo 8 a exatamente um dos elementos 1,3,5 e 7. Temos, na realidade que

$$\begin{aligned} 5\times1 &\equiv 5 \pmod 8 \\ 5\times3 &\equiv 7 \pmod 8 \\ 5\times5 &\equiv 1 \pmod 8 \\ 5\times7 &\equiv 3 \pmod 8. \end{aligned}$$

Multiplicando-se, membro a membro, estas congruências obtemos

$$5^4(1\times3\times5\times7) \equiv (1\times3\times5\times7) \pmod 8.$$

Como $(1\times3\times5\times7, 8) = 1$ podemos cancelar o fator $(1\times3\times5\times7)$ obtendo

$$5^4 \equiv 1 \pmod 8.$$

Observe que $4 = \phi(8)$, ou seja, provamos que $5^{\phi(8)} \equiv 1 \pmod 8$.

Teorema 2.13 (Euler) *Se m é um inteiro positivo e a um inteiro com $(a, m) = 1$, então*

$$a^{\phi(m)} \equiv 1 \pmod m.$$

Demonstração: No Teorema 2.12 mostramos que os elementos $ar_1, ar_2, \ldots, ar_{\phi(m)}$ constituem um sistema reduzido de resíduos módulo m se $(a, m) = 1$ e $r_1, r_2, \ldots, r_{\phi(m)}$ for um sistema reduzido de resíduos módulo m. Isto significa que ar_i é congruente a exatamente um dos, r_j $1 \le j \le \phi(m)$, e portanto o produto dos ar_i deve ser congruente ao produto dos r_j módulo m, isto é,

$$ar_1.ar_2\cdots ar_{\phi(m)} \equiv r_1.r_2.\ldots.r_{\phi(m)} \pmod m$$

ou seja

$$a^{\phi(m)}r_1.r_2\ldots r_{\phi(m)} \equiv r_1.r_2\ldots r_{\phi(m)} \pmod m.$$

Como

$$\left(\prod_{i=1}^{\phi(m)} r_i, m\right) = 1$$

podemos cancelar

$$\prod_{i=1}^{\phi(m)} r_i$$

em ambos os lados para obter $a^{\phi(m)} \equiv 1 (\text{mod } m)$. □

Como para p primo, $\phi(p) = p - 1$, o teorema acima é uma generalização do Teorema 2.11.

2.4 O Teorema do Resto Chinês

O nome dado ao teorema seguinte se deve ao fato de que este resultado já era conhecido, na antigüidade, pelos matemáticos chineses.

Teorema 2.14 (O Teorema do Resto Chinês) *Se* $(a_i, m_i) = 1$, $(m_i, m_j) = 1$ *para* $i \neq j$ *e* c_i *inteiro, então o sistema*

$$\begin{aligned} a_1x &\equiv c_1 (\text{mod } m_1) \\ a_2x &\equiv c_2 (\text{mod } m_2) \\ a_3x &\equiv c_3 (\text{mod } m_3) \\ &\vdots \\ a_rx &\equiv c_r (\text{mod } m_r) \end{aligned}$$

possui solução e a solução é única módulo m, *onde* $m = m_1 \cdot m_2 \cdots m_r$.

Demonstração: Do fato de $(a_i, m_i) = 1$, o Teorema 2.8 nos diz que $a_ix \equiv c_i (\text{mod } m_i)$ possui uma única solução que denotamos por b_i. Se definirmos $y_i = m/m_i$ onde, $m = m_1 \cdot m_2 \cdots m_r$, teremos $(y_i, m_i) = 1$, uma vez que $(m_i, m_j) = 1$ para $i \neq j$. Novamente, o Teorema 2.8 nos garante que cada uma das congruências $y_ix \equiv 1 (\text{mod } m_i)$ possui uma única solução que denotamos por $\overline{y}_i$. Logo, $y_i\overline{y}_i \equiv 1 (\text{mod } m_i)$, $i = 1, 2, \ldots, r$. Afirmamos que o número x dado por

$$x = b_1y_1\overline{y}_1 + b_2y_2\overline{y}_2 + \cdots + b_ry_r\overline{y}_r$$

é uma solução simultânea para o nosso sistema de congruências. De fato

$$\begin{aligned} a_ix &= a_ib_1y_1\overline{y}_1 + a_ib_2y_2\overline{y}_2 + \cdots + a_ib_iy_i\overline{y}_i + \cdots + a_ib_ry_r\overline{y}_r \\ &\equiv a_ib_iy_i\overline{y}_i (\text{mod } m_i) \equiv a_ib_i \equiv c_i (\text{mod } m_i) \end{aligned}$$

uma vez que y_j é divisível por m_i para $i \neq j$, $y_i\overline{y}_i \equiv 1 (\text{mod } m_i)$ e b_i é solução de $a_ix \equiv c_i (\text{mod } m_i)$.

Provamos, a seguir, que esta solução é única módulo m. Se $\overline{x}$ é uma outra solução para o nosso sistema, então $a_i\overline{x} \equiv c_i \equiv a_ix (\text{mod } m_i)$ e, sendo $(a_i, m_i) = 1$ obtemos $\overline{x} \equiv x (\text{mod } m_i)$. Logo $m_i | (\overline{x} - x)$, $i = 1, 2, \ldots, r$. Mas, como $(m_i, m_j) = 1$ para $i \neq j$ temos que

$$[m_1, m_2, \ldots, m_r] = m_1.m_2. \ldots .m_r.$$

Portanto, pelo Teorema 2.6, $m_1.m_2. \ldots .m_r | (\overline{x} - x)$, ou seja $\overline{x} \equiv x (\text{mod } m)$, o que conclui a demonstração. □

Mostramos, a seguir, um teste de divisibilidade, comum, para 7, 11 e 13.

Observando que $7 \times 11 \times 13 = 1001$ e que $10^3 = 1000 \equiv -1$ (mod 1001) temos

$$\begin{aligned} (a_ka_{k-1}a_{k-2} \ldots a_0)_{10} &= a_k10^k + a_{k-1}10^{k-1} + \ldots + a_110 + a_0 = \\ &= (10^2a_2 + 10a_1 + a_0) + +10^3(10^2a_5 + 10a_4 + a_3) + \\ &\quad + (10^3)^2(10^2a_8 + 10a_7 + a_6) + \cdots \\ &\equiv (a_2a_1a_0)_{10} - (a_5a_4a_3)_{10} + (a_8a_7a_6)_{10} - \cdots (\text{mod } 1001) \end{aligned}$$

Isto nos diz que um inteiro é congruente, módulo 1001, ao inteiro formado por sucessivamente, somando-se e subtraindo-se inteiros de três digitos formados por sucessivos blocos de três digitos, onde os digitos são agrupados começando-se pela direita.

Exemplo 2.5. Testar se os números 465647 e 2210000 são divisíveis por 7,11 ou 13.

Para o número 465647 temos: $647 - 465 = 182$.

Como $7|182, 11\nmid 182$ e $13|182$ concluimos que 465647 é divisível por 7 e 13 mas não por 11.

Para o número 2210000 temos: $000 - 210 + 2 = -208$.

Como $7\nmid 208, 11\nmid 208$ e $13|208$ concluimos que 2210000 é divisível por 13 mas não é divisível por 7 e nem por 11.

2.5 Problemas Resolvidos

Problema 2.1 Usando o Teorema de Wilson, encontrar o menor resíduo positivo de: a) $6 \times 7 \times 8 \times 9$ módulo 5 b) $8 \times 9 \times 10 \times 11 \times 12 \times 13$ módulo 7.

Solução: a) Para acharmos o menor resíduo positivo de $6 \times 7 \times 8 \times 9$, utilizamos o fato, elementar, de que $6 \equiv 1 (\text{mod } 5), 7 \equiv 2 (\text{mod } 5)$, $8 \equiv 3 (\text{mod } 5)$ e $9 \equiv 4 (\text{mod } 5)$. Logo,

$$6 \times 7 \times 8 \times 9 \equiv 1 \times 2 \times 3 \times 4 (\text{mod } 5)$$

e, pelo Teorema de Wilson sendo $4! \equiv -1 (\text{mod } 5)$, temos

$$6 \times 7 \times 8 \times 9 \equiv -1 \equiv 4 (\text{mod } 5).$$

b)·O menor resíduo positivo de $8 \times 9 \times 10 \times 11 \times 12 \times 13$ módulo 7 pode ser encontrado de forma análoga, isto é,

$$8 \times 9 \times 10 \times 11 \times 12 \times 13 \equiv 1 \times 2 \times 3 \times 4 \times 5 \times 6 (\text{mod } 7)$$

e, como $6! \equiv -1 \equiv 6(\text{mod } 7)$, temos que $8 \times 9 \times 10 \times 11 \times 12 \times 13 \equiv 6(\text{mod } 7)$.

Problema 2.2 Usando o Pequeno Teorema de Fermat , encontrar o resto da divisão de 2^{100000} por 17.

Solução: Pelo Teorema de Fermat temos $a^{p-1} \equiv 1(\text{mod } p)$ quando p é primo e $p \not| a$. Logo, como 17 é primo e $17 \not| 2$, temos $2^{16} \equiv 1(\text{mod } 17)$. Mas $100000 = 6250 \times 16$ e, portanto,

$$2^{100000} = (2^{16})^{6250} \equiv 1^{6250} \equiv 1(\text{mod } 17).$$

Logo, o resto da divisão por 17 de 2^{100000} é 1.

Problema 2.3 Encontrar o dígito das unidades de 3^{100} quando expresso na base 7.

Solução: Isto equivale a encontrar o menor resíduo positivo de 3^{100} módulo 7. Como 7 é primo e $7 \not| 3$, temos $3^6 \equiv 1(\text{mod } 7)$. Sendo $100 = 6 \times 16 + 4$, temos: $3^{96} = (3^6)^{16} \equiv (1)^{16} \equiv 1(\text{mod } 7)$. Agora, $3^2 = 9 \equiv 2(\text{mod } 7)$ e, portanto, $3^4 \equiv 4(\text{mod } 7)$. Assim $3^{100} = 3^{96} \times 3^4 \equiv 1 \times 4 \equiv 4(\text{mod } 7)$.

Problema 2.4 Mostrar que se p é um primo ímpar, então

$$2(p-3)! \equiv -1(\text{mod } p).$$

Solução: Sendo p primo, temos, pelo Teorema de Wilson que

$$(p-1)! \equiv -1(\text{mod } p)$$

mas, $(p-1)! = (p-1)(p-2)(p-3)!$ e, como $p-1 \equiv -1(\text{mod } p)$ e $p-2 \equiv -2(\text{mod } p)$ para $p \neq 2$, temos $(p-1)(p-2)(p-3)! \equiv (-1)(-2)(p-3)! \equiv 2(p-3)! \equiv -1(\text{mod } p)$.

Problema 2.5 Mostrar que se p e q são primos distintos, então

$$p^{q-1} + q^{p-1} \equiv 1(\text{mod } pq).$$

Solução: Devemos mostrar que $q|(p^{q-1} + q^{p-1} - 1)$ e que $p|(p^{q-1} + q^{p-1} - 1)$. Como $(q, p) = 1$ temos, pelo Teorema 2.11, que $q^{p-1} \equiv 1(\text{mod } p)$ e que $p^{q-1} \equiv 1(\text{mod } q)$. Logo, $p|(q^{p-1} - 1)$ e $q|(p^{q-1} - 1)$. Portanto, como $p|p^{q-1}$ e $q|q^{p-1}$, temos que $p|(p^{q-1} + q^{p-1} - 1)$ e que $q|(p^{q-1} + q^{p-1} - 1)$, o que conclui a demonstração.

Problema 2.6 Mostre que p é o menor primo que divide $(p-1)! + 1$.

Solução: Pelo Teorema de Wilson $p|((p-1)! + 1)$. Logo, como qualquer primo menor que p divide $(p-1)!$, nenhum deles pode dividir $(p-1)! + 1$ pois, neste caso, deveria dividir 1. Portanto, p é o menor primo tendo esta propriedade.

Problema 2.7 Mostrar que 2,3,5,7 e 13 são divisores de $n^{13} - n$ para todo n.

Solução: Como $n^{13} - n = n(n^{12} - 1)$ e

$$\begin{aligned}
n^{12} - 1 &= (n-1)(n^{11} + n^{10} + \cdots + n + 1) \\
n^{12} - 1 &= (n^2 - 1)(n^{10} + n^8 + \cdots + n^2 + 1) \\
n^{12} - 1 &= (n^4 - 1)(n^8 + n^4 + 1) \\
n^{12} - 1 &= (n^6 - 1)(n^6 + 1)
\end{aligned}$$

temos que $n, (n-1), (n^2-1), (n^4-1), (n^6-1)$ e $(n^{12}-1)$ são divisores de $n^{13} - n$. Logo, $2|(n^{13} - n)$ pois $n(n-1)$ é divisível por 2 e caso n não seja divisível por 3,5,7 e 13 teremos que

$$\begin{array}{llcll}
3|(n^{13}-n) & \text{pois } n^2 & \equiv & 1(\text{mod } 3) & \text{(Euler)} \\
5|(n^{13}-n) & \text{pois } n^4 & \equiv & 1(\text{mod } 5) & \text{(Euler)} \\
7|(n^{13}-n) & \text{pois } n^6 & \equiv & 1(\text{mod } 7) & \text{(Euler)} \\
13|(n^{13}-n) & \text{pois } n^{12} & \equiv & 1(\text{mod } 13) & \text{(Euler)}.
\end{array}$$

Problema 2.8 *Mostre que* $13|2^{70} + 3^{70}$.

Solução: Como $2^{12} \equiv 1(\text{mod } 13)$, temos que $2^{60} \equiv 1(\text{mod } 13)$. Mas $2^5 \equiv 6(\text{mod } 13)$ e, portanto, $2^{10} \equiv 36 \equiv -3(\text{mod } 13)$. Logo, $2^{60}.2^{10} \equiv -3(\text{mod } 13)$. Sabemos que $3^3 \equiv 1(\text{mod } 13)$, donde $3^{69} \equiv 1(\text{mod } 13)$. Como $3 \equiv 3(\text{mod } 13)$ temos que $3^{70} \equiv 3(\text{mod } 13)$. Logo somando-se, membro a membro, $2^{70} \equiv -3(\text{mod } 13)$ com $3^{70} \equiv 3(\text{mod } 13)$ obtemos $2^{70} + 3^{70} \equiv 0(\text{mod } 13)$, o que conclui a demonstração.

Problema 2.9 Mostrar que os números $1^2, 2^2, 3^2, \ldots, m^2, m > 2$, não formam um sistema completo de resíduos módulo m.

Solução: Basta mostrarmos que eles não são, dois a dois, incongruentes módulo m. Para isto é suficiente tomarmos dois números n e $k, n > k$, tais que

$n + k = m$, pois, desta forma

$$n^2 - k^2 = (n+k)(n-k) = m(n-k) \equiv 0 \pmod{m},$$

o que implica $n^2 \equiv k^2 \pmod{m}$, o que conclui a demonstração.

Problema 2.10 *Mostrar que para qualquer sistema reduzido* $r_1, r_2, \ldots, r_{p-1}$ *de resíduos módulo* p *(*p *primo), temos*

$$\prod_{i=1}^{p-1} r_i \equiv -1 \pmod{p}.$$

Solução: Sabemos que os números $1, 2, 3, \ldots, p-1$ formam um sistema reduzido de resíduos módulo p, para p primo. Isto significa que eles são todos primos com p e incongruentes módulo p. Logo, qualquer número relativamente primo com p é congruente módulo p a exatamente um destes números e, se dois números, primos com p, são incongrentes módulo p, eles serão congruentes a diferentes elementos deste conjunto. Portanto os números $r_1, r_2, \ldots, r_{p-1}$ são congruentes, módulo p, a diferentes elementos dentre $1, 2, \ldots, p-1$. Se multiplicarmos, membro a membro, estas congruências, teremos

$$\prod_{i=1}^{p-1} r_i \equiv 1 \times 2 \cdots (p-1) \equiv (p-1)! \pmod{p}$$

e, pelo Teorema de Wilson, o resultado segue, i.e.,

$$\prod_{i=1}^{p-1} r_i \equiv -1 \pmod{p}.$$

Problema 2.11 Mostrar que se p é um primo ímpar, então

$$1^2 \times 3^2 \times 5^2 \cdots (p-2)^2 \equiv (-1)^{(p+1)/2} \pmod{p}$$

e

$$2^2 \times 4^2 \times 6^2 \cdots (p-1)^2 \equiv (-1)^{(p+1)/2} \pmod{p}.$$

Solução: Mostramos apenas a primeira congruência, pois a segunda é análoga. Sabemos, pelo Teorema de Wilson, que

$$1 \times 2 \times 3 \times 4 \cdots (p-3)(p-2)(p-1) \equiv -1 \pmod{p}.$$

Substituímos $2, 4, 6, \ldots, (p-1)$, respectivamente, por $-(p-2), -(p-4), \ldots, -1$, obtendo

$$(-1)^{(p-1)/2} 1(p-2)3(p-4)5(p-6) \cdots 3(p-2)1 \equiv (-1) \pmod{p},$$

uma vez que, de 1 até $(p-1)$ temos $(p-1)/2$ pares. Como p é ímpar, todos os fatores acima são ímpares e cada um aparece duas vezes, logo

$$(-1)^{(p-1)/2} 1^2 \times 3^2 \times 5^2 \cdots (p-2)^2 \equiv -1 \pmod{p}.$$

Agora basta multiplicarmos, ambos os lados, por $(-1)^{(p-1)/2}$, o que conclui a demonstração.

Problema 2.12 Resolver o sistema de congruências abaixo:

$$\begin{aligned} x &\equiv 1 \pmod{5} \\ x &\equiv 2 \pmod{7} \\ x &\equiv 3 \pmod{11} \end{aligned}$$

Solução: Utilizando a notação introduzida no Teorema 2.14 temos:

$$\begin{aligned} &m_1 = 5; m_2 = 7; m_3 = 11, m = 5 \times 7 \times 11 \\ &y_1 = m/m_1 = 7 \times 11; y_2 = m/m_2 = 5 \times 11; y_3 = m/m_3 = 5 \times 7 \end{aligned}$$

Para determinar $\overline{y}_1$ resolvemos

$$\begin{aligned} &y_1 x \equiv 1 \pmod{m_1}, \text{ i.e.,} \\ &7 \times 11x \equiv 1 \pmod{5}, \text{ ou, equivalentemente} \\ &2x \equiv 1 \pmod{5}. \text{ Logo } \overline{y}_1 = 3 \end{aligned}$$

Encontramos $\overline{y}_2$ resolvendo

$$\begin{aligned} &y_2 x \equiv 1 \pmod{m_2}, \text{ i.e.,} \\ &5 \times 11x \equiv 1 \pmod{7}, \text{ ou, equivalentemente} \\ &6x \equiv 1 \pmod{7}. \text{ Logo } \overline{y}_2 = 6 \end{aligned}$$

Resolvendo $y_3 x \equiv 1 \pmod{m_3}$ obtemos $\overline{y}_3$:

$$\begin{aligned} &5 \times 7x \equiv 1 \pmod{11}, \text{ i.e.,} \\ &2x \equiv 1 \pmod{11} \end{aligned}$$

e, portanto, $\overline{y}_3 = 6$.

Como, neste caso, $b_1 = 1, b_2 = 2$ e $b_3 = 3$ temos que a solução do sistema módulo 5×7×11 é dada por

$$\begin{aligned} x &\equiv b_1y_1\overline{y}_1 + b_2y_2\overline{y}_2 + b_3y_3\overline{y}_3 \\ &\equiv 1 \times 7 \times 11 \times 3 + 2 \times 5 \times 11 \times 6 + 3 \times 5 \times 7 \times 6 \\ &\equiv 366 \pmod{385} \end{aligned}$$

Problema 2.13 Mostrar que $\sqrt[n]{k}$ é um irracional onde k não é a n-ésima potência de um inteiro.

Solução: Vamos supor que $\sqrt[n]{k}$ seja racional, isto é, que existam inteiros a e b, com $\sqrt[n]{k} = a/b$, isto é, $a^n = kb^n$. Como k não é uma n-ésima potência de um inteiro, ele deve ter algum fator primo p cuja multiplicidade não é congruente a $0 \pmod{n}$. Como a multiplicidade de p e de todos os outros fatores primos em b^n é congruente a $0 \pmod{n}$ concluímos que a múltiplicidade de p em kb^n não é congruente a $0 \pmod{n}$. Mas, como a multiplicidade de p em a^n claramente é congruente a $0 \pmod{n}$ temos uma contradição, isto é, $kb^n \neq a^n$. Desta forma $\sqrt[n]{k}$ é racional somente quando k é uma n-ésima potência de um inteiro. □

Observe que contrário às provas de casos especiais deste resultado, como o da irracionalidade de $\sqrt{2}$, neste argumento não é necessário supor que a e b sejam relativamente primos.

2.6 Problemas Propostos

1. Mostrar que $47|(2^{23} - 1)$.

2. Encontrar o resto da divisão de 7^{34} por 51 e o resto da divisão de 5^{63} por 29.

3. Mostrar que se p é um ímpar e $a^2+2b^2 = 2p$, então "a"é par e "b"é ímpar.

4. Provar que para p primo $(p-1)! \equiv p - 1 \pmod{1 + 2 + 3 + \ldots + (p-1)}$.

5. Encontrar o máximo divisor comum de $(p-1)! - 1$ e $p!$ (p primo).

6. Mostrar que para $n \geq 4$ o resto da divisão por 12 de $1! + 2! + 3! + \ldots + n!$ é 9.

7. Mostrar que para n inteiro $3n^2 - 1$ nunca é um quadrado.

8. Resolver as seguintes congruências.
(a) $5x \equiv 3 \pmod{24}$
(b) $3x \equiv 1 \pmod{10}$

(c) $23x \equiv 7 \pmod{19}$
(d) $7x \equiv 5 \pmod{18}$
(e) $25x \equiv 15 \pmod{120}$

9. Mostrar que $5n^3 + 7n^5 \equiv 0 \pmod{12}$ para todo inteiro n.

10. Seja $f(x) = a_0 + a_1x + \ldots + a_nx^n$ um polinômio com coeficientes inteiros onde $a_n > 0$ e $n \geq 1$. Mostrar que $f(x)$ é composto para infinitos valores da variável x.

11. Mostrar que se p_1 e p_2 são primos tais que $p_2 = p_1 + 2$ e $p_1 > 3$, então $p_1 + p_2 \equiv 0 \pmod{12}$.

12. Mostrar que para a e b inteiros temos que $3|(a^2 + b^2) \Rightarrow 3|a$ e $3|b$.

13. Sejam p_1, p_2 e p_3 primos tais que $p = p_1^2 + p_2^2 + p_3^2$ é primo. Mostrar que algum dos $p_i's$ é igual a 3.

14. Mostrar que $3x^2 + 4x^2 \equiv 3 \pmod{5}$ é equivalente a $3x^2 - x^2 + 2 \equiv 0 \pmod{5}$.

15. Mostrar que $p|\binom{p^\alpha}{k}$ onde $0 < k < p^\alpha$.

16. Seja p primo e M um conjunto de p inteiros consecutivos. É possível encontrar M_1 e M_2 subconjuntos de M tais que $M_1 \cup M_2 = M, M_1 \cap M_2 = \phi, M_i \neq \phi$ de forma que

$$\prod_{i \in M_1} i = \prod_{j \in M_2} j?$$

17. Seja f(x) um polinômio com coeficientes inteiros. Mostrar que se $f(-1), f(0)$ e $f(1)$ não são divisíveis por 3, então $f(n) \neq 0$ para todo inteiro n.

18. Mostrar que $3^{10} \equiv 1 \pmod{11^2}$.

19. Resolver os seguintes sistemas:

a) $\begin{cases} x \equiv 1 \pmod{2} \\ x \equiv 2 \pmod{3} \\ x \equiv 5 \pmod{7} \end{cases}$ b) $\begin{cases} 2x \equiv 1 \pmod{5} \\ 3x \equiv 2 \pmod{7} \\ 5x \equiv 7 \pmod{11} \end{cases}$ c) $\begin{cases} x \equiv 7 \pmod{11} \\ 3x \equiv 5 \pmod{13} \\ 7x \equiv 4 \pmod{5} \end{cases}$

20. Encontrar todas as soluções de cada uma das seguintes congruências lineares. (a) $5x \equiv 3 \pmod{7}$
(b) $13x \equiv 14 \pmod{29}$
(c) $15x \equiv 9 \pmod{25}$
(d) $37x \equiv 16 \pmod{19}$
(e) $5x \equiv 20 \pmod{15}$

21. Mostrar que $a^7 \equiv a \pmod{21}$ para todo inteiro a.

22. Mostrar que para a e b inteiros, com $(a, b) = 1$ temos:

$$a^{\phi(b)} + b^{\phi(a)} \equiv 1 \pmod{ab}$$

23. Provar ou dar contra-exemplo: "Se a e m são inteiros $(a, m) = 1$, então

$$m|(1 + a + a^2 + \ldots + a^{\phi(m)-1})".$$

24. Mostrar que se p e q são primos, $p \geq q \geq 5$, então $p^2 - q^2 \equiv 0 \pmod{24}$.

25. Encontrar um sistema completo de resíduos módulo 11 formado somente por múltiplos de 6.

26. Encontrar um sistema completo de resíduos módulo 7 onde todos os elementos são números primos.

27. Dado um primo p é sempre possível encontrar um sistema completo de resíduos módulo p formado só por primos? Justificar.

28. Provar que, para todo número composto $n, n \neq 4$, a congruência $(n-1)! \equiv 0 \pmod{n}$ é verdadeira.

Capítulo 3

Teoria Combinatória dos Números

3.1 Princípio da Casa dos Pombos

Embora este tópico apareça, com mais freqüência, em livros de Combinatória, ele não deixa de ser parte da Teoria dos Números. Mesmo em se tratando de algo simples, esta idéia auxilia na demonstração de muitos resultados não-triviais, como os problemas abaixo poderão mostrar.

O *Princípio da Casa dos Pombos* nos diz que para colocarmos $n+1$ pombos em n gaiolas, pelo menos uma gaiola deverá conter pelo menos dois pombos. Esta idéia tão óbvia é, na realidade, uma poderosa ferramenta na demonstração de muitos resultados bastante difíceis. O que, muitas vezes, torna o problema difícil é a construção de um conjunto ou conjuntos aos quais se possa aplicar este princípio.

Este princípio é também conhecido como "Princípio das Gavetas de Dirichlet" por ter sido por ele enunciado como: "Se $n + 1$ objetos são colocados em n gavetas, então pelo menos uma gaveta deverá conter, pelo menos, dois objetos".

Nos exemplos apresentados a seguir, utilizamos, várias vezes, resultados do Capítulo 2 sobre congruências.

Exemplo 3.1. Mostrar que, numa festa de aniversário com mais de 12 crianças, existem pelo menos duas nascidas no mesmo mês e que também existem pelo menos duas nascidas no mesmo dia da semana.

Como temos mais crianças (pombos) do que meses (gaiolas), pelo menos um "mês"deverá conter pelo menos duas "crianças". Na segunda parte, sendo o número de crianças maior do que 7, necessariamente duas ou mais terão nascido no mesmo dia da semana.

Exemplo 3.2. Mostrar que todo subconjunto de $\{1, 2, 3, \ldots, 2n\}$, contendo $n+1$ elementos, possui um par de elementos primos entre si.

É fácil observar que os únicos subconjuntos de $\{1, 2, \ldots, 2n\}$ contendo n elementos, não-consecutivos, são $\{1, 3, 5, \ldots, 2n-1\}$ e $\{2, 4, 6, \ldots, 2n\}$. Portanto, ao tomarmos um subconjunto com $n+1$ elementos teremos, necessariamente, dois elementos consecutivos que, sendo primos entre si, irão garantir nosso resultado.

Exemplo 3.3. Mostrar que o subconjunto do problema anterior também contém um par de elementos tais que um é múltiplo do outro.

Sabemos que todo inteiro n pode ser escrito na forma $n = 2^r m$, onde $r \geq 0$ e m ímpar. Como em $\{1, 2, 3, \ldots, 2n\}$ existem apenas n ímpares distintos, quando tomarmos $n+1$ deste números, pelo menos dois deles terão o mesmo m quando representados na forma $2^r m$. Um deles será $2^s m$ e o outro $2^r m$. E é claro que um destes divide o outro.

Exemplo 3.4. Mostrar que qualquer subconjunto S de $\{1, 2, 3, \ldots, 12\}$ contendo sete elementos possui dois subconjuntos cuja soma dos elementos é a mesma.

Um subconjunto com 7 elementos terá soma no máximo igual a $6+7+8+9+10+11+12 = 63$. Disto concluímos que os possíveis valores para a soma dos elementos de um subconjunto de um conjunto contendo 7 dos elementos de $\{1, 2, 3, \ldots, 12\}$ vão de 1 a 63, ou seja, temos 63 valores possíveis. Mas um conjunto com 7 elementos possui $2^7 - 1$ subconjuntos não-vazios. Logo, como $2^7 - 1 > 63$, pelo menos dois deles terão a mesma soma para os seus elementos.

Exemplo 3.5. Mostrar que em um conjunto de m elementos, $a_1, a_2, \ldots, a_m$, tais que $a_i \not\equiv 1 (\text{mod } m), i = 1, 2, 3, \ldots, m$, existem pelo menos dois cuja diferença é divisível por m.

Sabemos que os elementos $0, 1, 2, \ldots, m-1$, formam um sistema completo de resíduos módulo m. A restrição $a_i \not\equiv 1 (\text{mod } m)$ nos diz que nenhum dos a_i's está na classe à qual 1 pertence. Portanto temos $m-1$ classes para colocarmos os m a_i's, o que nos garante que pelo menos dois deles deverão estar na mesma classe, o que conclui a demonstração.

□

Exemplo 3.6. Mostrar que, dentre 9 pontos quaisquer de um cubo de aresta 2, existem pelo menos dois pontos que se encontram a uma distância menor do que ou igual a $\sqrt{3}$ um do outro.

Dividimos este cubo em oito cubos menores dividindo cada aresta ao meio. Cada um dos 8 cubos assim gerados, tendo aresta 1, terá diâmetro igual a $\sqrt{3}$. Como temos 9 pontos, pelo menos um dos 8 cubos conterá 2 pontos, o que conclui a demonstração.

Exemplo 3.7. Seja B um conjunto contendo k elementos relativamente primos com m. Mostrar que, se $k > \phi(m)$ então B possui pelo menos dois elementos

cuja diferença é divisível por m.

Como um sistema reduzido de resíduos módulo m contém $\phi(m)$ elementos e $k > \phi(m)$, pelo menos 2 deverão ficar na mesma classe de congruência módulo m, uma vez que todos são primos com m. Observe que um número primo com m deverá, necessariamente, pertencer a uma classe de congruência cujo representante é primo com m.

Exemplo 3.8. Suponhamos que os números de 1 até 15 sejam distribuídos de modo aleatório em torno de um círculo. Mostrar que a soma dos elementos de pelo menos um conjunto de 5 elementos consecutivos, tem que ser maior do que ou igual a 40.

Observe que, se somarmos todos os possíveis conjuntos de 5 elementos consecutivos (são 15), cada um dos números de 1 a 15 terá sido somado 5 vezes e que, portanto, a soma total será $5(1+2+3+\cdots+15) = 5(15+1)15/2 = 600$. Como são 15 conjuntos distintos de 5 elementos consecutivos, se cada um tiver soma inferior a 40, o total será no máximo $15 \times 39 = 585$. Logo, pelo menos um deve ter soma maior do que ou igual a 40.

Exemplo 3.9. Mostrar que todo inteiro positivo n possui um múltiplo que se escreve na base 10, somente com os dígitos 0 e 1.

Basta considerarmos a sequência dos $n+1$ números $1, 11, 111, 1111, \ldots, 11\ldots1$, onde o último contém $n+1$ "1". Como temos mais números nesta lista do que o número de classes incongruentes módulo n, pelo menos dois deles estarão na mesma classe. Logo, a diferença será divisível por n. É fácil ver que a diferença de elementos da seqüência acima contém somente zeros e uns.

Exemplo 3.10. Um indivíduo estuda pelo menos uma hora por dia durante 5 semanas, mas nunca estuda mais do que 11 horas em 7 dias consecutivos. Mostrar que, em algum período de dias sucessivos, ele estuda um total de exatamente 20 horas. (Admita que ele estude um número inteiro de horas por dia).

Seja d_i o número de horas que ele estudou no dia i. São 35 dias. Consideremos a sequência

$$
\begin{aligned}
b_1 &= d_1 \\
b_2 &= d_1 + d_2 \\
b_3 &= d_1 + d_2 + d_3 \\
&\vdots \\
b_{21} &= d_1 + d_2 + d_3 + \cdots + d_{21}.
\end{aligned}
$$

Como temos 21 números distintos, dois deles, pelo menos, estarão na mesma classe de congruência módulo 20. Logo a diferença entre eles deve ser múltipla de 20. Como, num período de 21 dias, ele poderá ter estudado no máximo 33 horas (3×11), esta diferença, não sendo nula, terá que ser exatamente igual a 20, o que conclui a demonstração.

Exemplo 3.11. Seja S um conjunto contendo k inteiros tais que nenhum deles é múltiplo de m. Para $k > m/2$ mostrar que existem dois inteiros em S cuja soma ou diferença é divisível por m.

Observe que se m for par ou ímpar, isto é, $m = 2n$ ou $m = 2n + 1$ nós temos, em ambos os casos, que $k \geq n+1$. Consideremos, agora, os n conjuntos $S_1, S_2, \ldots, S_n$ onde S_i contém todos os elementos de S congruentes a i ou $-i$ módulo m. Como temos n conjuntos e $k \geq n + 1$ pelo menos um deles deverá conter pelo menos 2 dos elementos de S. Portanto a soma ou diferença destes dois elementos será múltipla de m.

□

3.2 Generalizações – Exemplos

O Princípio da Casa dos Pombos pode ser, de maneira mais geral, enunciado como:

Teorema 3.1. *Se n gaiolas são ocupadas por $nk + 1$ pombos, então pelo menos uma gaiola deverá conter pelo menos $k + 1$ pombos.*

Demonstração. Isto também é óbvio, pois se cada uma contiver no máximo k, como são n, no máximo nk terão sido distribuídos, o que é uma contradição. □

Exemplo 3.12. Numa festa de aniversário com 37 crianças, pelo menos 4 nasceram no mesmo mês.

Como $37 = 3 \cdot 12 + 1$ o resultado segue pelo Teorema 3.1 com $n = 12$ e $k = 3$.

Exemplo 3.13. Se uma urna contém 4 bolas vermelhas, 7 bolas verdes, 9 bolas azuis e 6 bolas amarelas, qual é o menor número de bolas que devemos retirar (sem olhar) para que possamos ter certeza de termos tirado pelo menos 3 de uma mesma cor?

Consideramos como gaiolas as 4 cores diferentes e, portanto, tomando $k = 2$ e $n = 4$ no Teorema 3.1, temos $4 \cdot 2 + 1 = 9$ para a resposta do nosso problema.

Exemplo 3.14. Num grupo de n pessoas ($n \geq 2$) existem pelo menos duas pessoas com o mesmo número de conhecidos. Neste e nos exemplos seguintes

assumimos que a relação de conhecimento é simétrica, isto é, se a conhece b, então b conhece a.

Vamos particionar estas n pessoas em subconjuntos $A_0, A_1, \ldots, A_{n-1}$, onde A_i é o subconjunto que contém as pessoas que conhecem i pessoas no grupo de n. Logo, se uma pessoa não conhece nenhuma outra das $n - 1$ pessoas ela estará no grupo A_0, se tem somente um conhecido estará em A_1 e assim por diante, até A_{n-1}, caso ela conheça todas as outras $n - 1$ pessoas. Mas se o subconjunto A_0 possui alguém, A_{n-1} não possui ninguém e vice-versa. Isto porque se alguém não conhece ninguém é porque ninguém conhece todos e se alguém conhece todos os outros não há ninguém que seja desconhecido de todos. Logo, as n pessoas estão particionadas em $n - 1$ subconjuntos e, portanto, algum subconjunto contém pelo menos duas pessoas, o que conclui a demonstração. □

No enunciado a seguir, utilizamos a notação $\lfloor x \rfloor$* para designar o *maior inteiro menor do que ou igual a* x. Podemos ver o teorema como uma reformulação do Princípio da Casa dos Pombos.

Teorema 3.2. *Se colocarmos em n gaiolas k pombos, então pelo menos uma gaiola deverá conter pelo menos $\left\lfloor \frac{k-1}{n} \right\rfloor + 1$ pombos.*

Demonstração. Como

$$\left\lfloor \frac{k-1}{n} \right\rfloor \leq \frac{k-1}{n},$$

se cada gaiola contiver no máximo $\left\lfloor \frac{k-1}{n} \right\rfloor$ pombos, teremos no máximo $n\left\lfloor \frac{k-1}{n} \right\rfloor$ pombos no total. Mas

$$n\left\lfloor \frac{k-1}{n} \right\rfloor \leq n\left(\frac{k-1}{n}\right) = k - 1 < k,$$

o que é uma contradição. □

Exemplo 3.15. Em qualquer grupo de 20 pessoas, pelo menos 3 nasceram no mesmo dia da semana.

No Teorema 3.2, tomamos $n = 7$ e $k = 20$. Logo, como

$$\left\lfloor \frac{20-1}{7} \right\rfloor + 1 = \left\lfloor \frac{19}{7} \right\rfloor + 1 = 2 + 1 = 3,$$

*Esta função será estudada no capítulo 4.

pelo menos 3 terão nascido no mesmo dia da semana. □

Exemplo 3.16. Suponhamos 6 pontos no espaço, não havendo 3 numa mesma linha. Cada dois pontos ligados por um segmento de reta e cada um desses 15 segmentos pintado de uma cor dentre duas: azul e vermelho. Provar que, qualquer que seja a escolha destas duas cores na pintura dos segmentos, sempre existirá um triângulo com todos os lados de uma mesma cor.

Qualquer ponto A está ligado a 5 outros por 5 segmentos de reta. Existem duas cores disponíveis para estes 5 segmentos, logo devemos ter pelo menos 3 segmentos com a mesma cor.

Desta forma, temos a Figura 3.1 onde os três segmentos partindo de A que são da mesma cor, suponhamos azul (representada pela linha sólida), vão para B, C e D. Considere o triângulo BCD. Se qualquer um de seus lados, BC por exemplo, é azul, então existe um triângulo azul, ABC. Se nenhum é azul, então BCD é um triângulo vermelho.

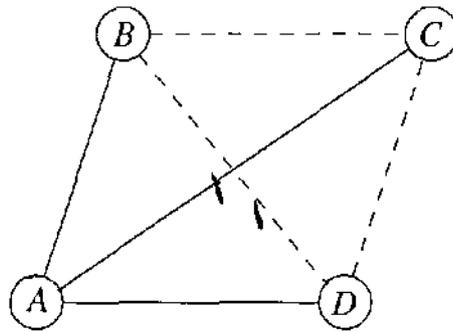



Figura 3.1

Exemplo 3.17. Em qualquer grupo de 6 pessoas existe, necessariamente, um conjunto de 3 pessoas que se conhecem ou que são totalmente estranhos.

Este problema é idêntico ao anterior, apenas se encontra com uma roupagem diferente. Basta identificarmos as pessoas com os pontos, a relação de conhecimento com os segmentos de uma das cores e o não-conhecimento recíproco como os segmentos da outra cor. □

No teorema seguinte apresentamos mais uma importante aplicação do Princípio da Casa dos Pombos, dada por Erdös e Szekeres [9].

Teorema 3.3. *Toda seqüência de n^2+1 inteiros diferentes possui uma subseqüência crescente de $n+1$ termos ou uma subseqüência decrescente de $n+1$ termos.*

Demonstração. Consideremos a sequência

$$a_1, a_2, a_3, \ldots, a_{n^2+1}.$$

Seja t_i o número de termos na mais longa subseqüência crescente começando em a_i. Se algum t_i for pelo menos $n+1$, o teorema estará demonstrado. Vamos, pois, assumir que $1 \leq t_i \leq n$, para todo i. Logo, como temos n^2+1 t_i's (pombos) para apenas n gaiolas (os números $1, 2, \ldots, n$), pelo Teorema 3.2 existe pelo menos uma gaiola contendo pelo menos

$$\left\lfloor \frac{n^2+1-1}{n} \right\rfloor + 1 = n+1$$

pombos. Isto é, existem pelo menos $n+1$ t_i's que são iguais. Vamos mostrar que os a_i's aos quais os t_i's estão associados formam uma subseqüência decrescente. Suponhamos $t_i = t_j$ com $i < j$. Devemos mostrar que $a_i > a_j$. Se $a_i \leq a_j$, teremos $a_i < a_j$, pois, por hipótese, todos os a_i's são diferentes. Logo a_i seguido pela maior subseqüência que começa em a_j forma uma subseqüência crescente de comprimento $t_j + 1$. Isto implica $t_i \geq t_j + 1$, o que é uma contradição. □

Como uma aplicação deste teorema vamos encontrar a subseqüência de comprimento 4 para a seqüência $9, 8, 4, 3, 2, 7, 6, 5, 10, 1$.

Os t_i's são:

$$t_1 = 2,\ t_2 = 2,\ t_3 = 3,\ t_4 = 3,\ t_5 = 3,$$
$$t_6 = 2,\ t_7 = 2,\ t_8 = 2,\ t_9 = 1,\ t_{10} = 1,$$

Existem 5 t_i's iguais a 2 (o teorema nos garante pelo menos 4) e quaisquer 4 (por exemplo t_1, t_2, t_6 e t_7) nos fornecem uma seqüência decrescente (neste caso 9, 8, 7, 6).

Exemplo 3.18. Provar que 7 divide infinitos números da forma 252525 ...25.

Consideremos primeiramente os oito números abaixo:

25
2525
252525
25252525
2525252525
252525252525
25252525252525
2525252525252525

Como temos mais do que 7 números, pelo menos dois deles estão na mesma classe de congruência módulo 7. Logo, a diferença entre eles é divisível por 7. Mas esta diferença é da forma

$$2525\ldots25\ldots0000 = 2525\ldots25 \cdot 10^{2k},$$

o que nos fornece um número divisível por 7 da forma desejada uma vez que o primo 7 não é um divisor de 10^{2k}.

A obtenção de um conjunto infinito pode ser facilmente obtida pela repetição do que foi feito, utilizando-se seqüências suficientemente grandes para se evitar repetições. □

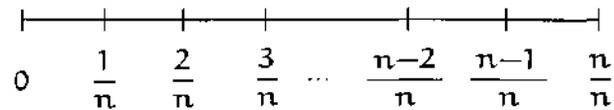
No teorema seguinte mostramos que o conjunto Q dos números racionais é *denso* no conjunto dos números reais[1].

Provaremos, na realidade, um resultado mais importante do que a simples densidade dos racionais. Mostraremos como obter uma seqüência infinita de aproximações, cada vez melhores, de um irracional, através de racionais p_i/q_i. No Capítulo 8, sobre frações contínuas, também descrevemos um processo de aproximações sucessivas de irracionais por racionais.

Teorema 3.4. *Mostrar que, dados $\alpha \in \mathbb{R}$ e $n > 1$, um inteiro, existe um racional $\frac{p}{q}$, onde $1 \leq q \leq n$, tal que*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{nq}. \tag{3.1}$$

Demonstração. Consideremos os $n+1$ números $0, \alpha - \lfloor\alpha\rfloor, 2\alpha - \lfloor 2\alpha\rfloor, \ldots, n\alpha - \lfloor n\alpha\rfloor$, e a seguinte divisão do intervalo $[0,1]$:

$$0 \quad \frac{1}{n} \quad \frac{2}{n} \quad \frac{3}{n} \quad \cdots \quad \frac{n-2}{n} \quad \frac{n-1}{n} \quad \frac{n}{n}$$

Como cada um dos $n+1$ números pertence ao intervalo $[0,1)$ e este intervalo está dividido nos n subintervalos de comprimento

$$\frac{1}{n}, [0,\frac{1}{n}), [\frac{1}{n},\frac{2}{n}), [\frac{2}{n},\frac{3}{n}), \ldots, [\frac{n-1}{n},\frac{n}{n}),$$

[1] Isto significa que dado qualquer real x existe um racional tão próximo de x quanto quisermos.

podemos concluir que existem s e t, $0 \leq s < t \leq n$, tais que $s\alpha - \lfloor s\alpha\rfloor$ e $t\alpha - \lfloor t\alpha\rfloor$ pertencem a um mesmo subintervalo.

Sejam $q = t - s$ e $p = \lfloor t\alpha\rfloor - \lfloor s\alpha\rfloor$. Temos, portanto,

$$\begin{aligned} |q\alpha - p| &= |(t-s)\alpha - (\lfloor t\alpha\rfloor - \lfloor s\alpha\rfloor)| \\ &= |(t\alpha - \lfloor t\alpha\rfloor) - (s\alpha - \lfloor s\alpha\rfloor)| \\ &< \frac{1}{n}. \end{aligned}$$

Logo $\left|\alpha - \frac{p}{q}\right| < \frac{1}{nq}$. □

Como em (3.1), $q \leq n$, temos, de fato, provado que

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2} \tag{3.2}$$

Em (3.1) e (3.2) podemos, obviamente, supor que p e q são relativamente primos. Se α for um racional, $\alpha = \frac{a}{b}$, onde $(a,b) = 1$ e $b > 0$, então a desigualdade (3.2) tem somente um número finito de soluções em números p e q relativamente primos pois, se $\alpha \neq \frac{p}{q}$ e $p > 0$, temos

$$\left|\alpha - \frac{p}{q}\right| = \left|\frac{a}{b} - \frac{p}{q}\right| = \frac{|aq - bp|}{bq} \geq \frac{1}{bq}.$$

donde concluímos que, sendo (3.2) verificado, $q < b$.

No teorema seguinte mostramos que (3.2) possui infinitas soluções para α um irracional.

Teorema 3.5. *Se α é um irracional, então a desigualdade (3.2) possui um número infinito de soluções em inteiros p e q relativamente primos.*

Demonstração: Seja n_1 um inteiro, $n_1 > 1$. Pelo Teorema 3.4 obtemos um par de inteiros p_1 e q_1, relativamente primos, tal que

$$\beta_1 = \left|\alpha - \frac{p_1}{q_1}\right| < \frac{1}{n_1 q_1}$$

onde $1 \leq q_1 \leq n_1$. Como α é irracional, $\beta_1 \neq 0$. Logo podemos escolher um inteiro $n_2 > \frac{1}{\beta_1}$ e determinar inteiros p_2 e q_2, relativamente primos, tais que

$$\beta_2 = \left|\alpha - \frac{p_2}{q_2}\right| < \frac{1}{n_2 q_2} \leq \frac{1}{n_2} < \beta_1$$

com $1 \leq q_2 \leq n_2$. Repetindo este procedimento, obtemos uma seqüência infinita decrescente de números positivos

$$\beta_1 > \beta_2 > \beta_3 > \cdots > \beta_i > \cdots$$

onde o número

$$\beta_i = \left|\alpha - \frac{p_i}{q_i}\right|$$

satisfaz a desigualdade $\beta_i < 1/q_i^2$, o que conclui a demonstração do teorema. □

No teorema seguinte apresentamos mais uma importante e simples conseqüência do Teorema 3.4.

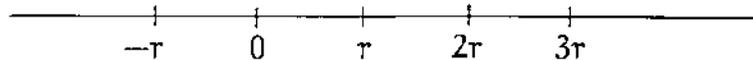
Teorema 3.6. *Para* α *um irracional o conjunto* $\{m+n\alpha, m, n \in \mathbb{Z}\}$ *é denso em* $\mathbb{R}$.

Demonstração. Devemos mostrar que para todo β real e $\varepsilon > 0$, arbitrário, existem inteiros m, n tais que $|\beta - (m + n\alpha)| < \varepsilon$.

Escolhamos, inicialmente, N tal que $\frac{1}{N} < \varepsilon$. Para este N e o α dado, o Teorema 3.4 nos garante a existência de inteiros p e q tais que

$$|q\alpha - p| < \frac{1}{N}.$$

Sendo α irracional, $|q\alpha - p| > 0$.

Podemos, desta forma, dividir a reta em multiplos de $r = |q\alpha - p|$.

donde concluímos que existe um inteiro M tal que $Mr \leq \beta < (M+1)r$. Logo

$$\begin{aligned} |\beta - Mr| &= |\beta - M(q\alpha - p)| \\ &= |\beta - ((-Mp) + (Mq)\alpha)| \\ &= |\beta - (m + n\alpha)| < \frac{1}{N} < \varepsilon. \end{aligned}$$

Na última seqüência de igualdades admitimos $r = q\alpha - p$. Para $r = p - q\alpha$ teríamos tomado $m = Mp$ e $n = -Mq$, o que conclui a demonstração. □

3.3 Demonstração Combinatória do Pequeno Teorema

A demonstração que apresentamos para o corolário do Teorema 2.11 segue Andrews [3].

Teorema 3.7. *Se* p *é um primo e "*n*" um inteiro positivo, então* $p|(n^p - n)$.

Demonstração: Suponhamos que nós desejamos formar correntes com p contas coloridas cada uma e que nós possuimos, em mãos, contas suficientes que nos permitem o uso ilimitado de cada uma das n cores. Quantas correntes diferentes podemos formar? Pelo Princípio Multiplicativo este número é, claramente, n^p uma vez que cada conta pode ser escolhida em, exatamente, n maneiras e são p escolhas para cada corrente. A Figura 3.2 ilustra o caso em que $n = 3$ e $p = 3$.

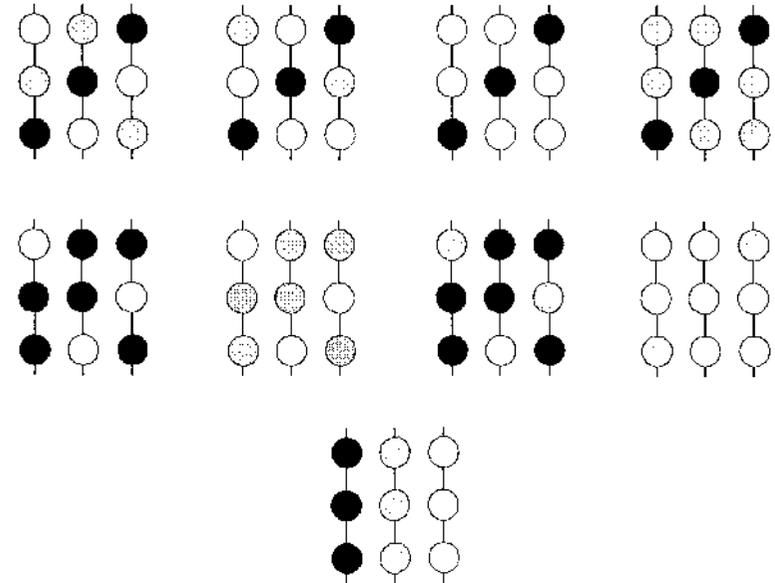



Figura 3.2

Das n^p possibilidades, exatamente n correntes possuem somente uma cor. Colocando estas à parte juntamos, da maneira ilustrada na Figura 3.3, as duas extremidades de cada uma das $n^p - n$ correntes formando $n^p - n$ braceletes.

Nós podemos alterar qualquer corrente de contas removendo uma conta da parte de cima e colocando-a na parte de baixo. Esta alteração produz uma corrente diferente sem alterar o bracelete resultante. Quando $n = 3$ e $p = 3$,

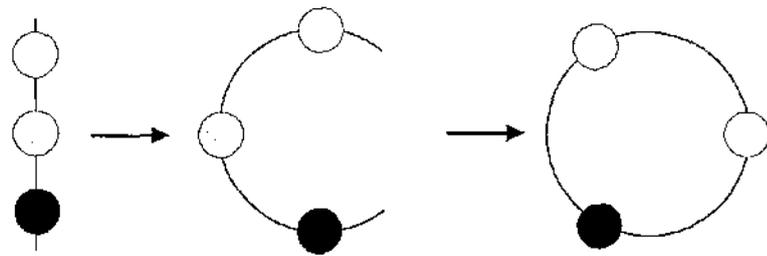



Figura 3.3

as 24 correntes multicoloridas se juntam, naturalmente, em 8 grupos de 3 correntes que podem ser obtidas, uma da outra, por uma ou mais repetições da alteração que descrevemos. Veja os oito primeiros grupos da Figura 3.2. Para cada um destes oito diferentes grupos corresponde um bracelete distinto (veja Figura 3.4).

Seja k o menor número de vezes que esta alteração pode ser repetida até que a corrente original seja reproduzida. Claramente $k > 1$, desde que nós separamos as correntes em que todas as contas são de uma mesma cor. Observe que após $2k$ alterações o bracelete original será reproduzido novamente e, de forma semelhante, após $3k, 4k$, etc. Pelo algoritmo da divisão de Euclides (Teorema 1.2) existem h e r tais que $p = hk + r \quad (0 \leq r < k)$.

Como uma corrente é reproduzida após hk passos (alterações) e é também reproduzida após p passos, serão necessários r passos, após o hk-ésimo passo para se obter uma reprodução da coloração inicial. Como $r < k$ e k é o menor número inteiro positivo de passos necessários para a obtenção de uma reprodução, vemos que r deve ser 0. Logo $p = hk$ e, portanto, $k = p$ uma vez que $k > 1$ e p é primo. Conseqüentemente, as $n^p - n$ correntes podem ser agrupadas em grupos de p correntes cada, e é claro que cada grupo gera um bracelete diferente.

Desta forma, o número de braceletes N multiplicado por p fornece o número de correntes que não são formadas de uma única cor, que é $n^p - n$. Logo, $pN = n^p - n$, isto é, $p | (n^p - n)$.

3.4 Demonstração Combinatória do Teorema de Wilson

No Capítulo 2 (Teorema 2.9) mostramos que para p primo a seguinte relação se verifica $(p-1)! \equiv -1 (\text{mod } p)$. Este resultado atribuido a Wilson (1741-1793) por E. Waring em *Meditaciones Algebraicae* (1770) já era conhecido de

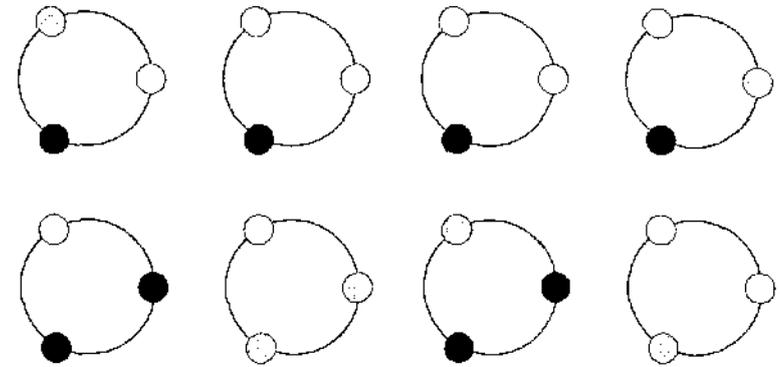



Figura 3.4

Leibnitz antes de 1683.

Apresentamos, a seguir, uma demonstração combinatória para este resultado seguindo Andrews [3].

Teorema 3.8. *Se* p *é primo, então* $(p-1)! \equiv -1 (\text{mod } p)$.

Demonstração. Isto é óbvio no caso $p = 2$. Podemos assumir, portanto, que p seja um primo ímpar. Consideramos p pontos em um círculo distribuídos de tal forma que eles dividem o círculo em p arcos iguais. Quantos são os polígonos que podemos formar unindo estes pontos (cruzamentos de arestas são permitidos). Estes polígonos são chamados p-ágonos estrelados pelo fato de seus vértices serem os vértices de um polígono regular convexo de p lados. É de se esperar que o total de tais polígonos seja $p!$ Isto porque temos p escolhas para o primeiro vértice, $(p-1)$ para o segundo e assim sucessivamente. Observe, entretanto, que podemos descrever cada um destes p-ágonos de $2p$ maneiras diferentes, isto é, iniciando em qualquer um dos p vértices e escolhendo uma ou outra das duas arestas naquele vértice como inicial. Portanto, nós obtemos, na realidade, $p!/2p$ diferentes p-ágonos.

A Figura 3.5 mostra os 12 pentágonos estrelados.

Dos $p!/2p$ p-ágonos, exatamente $(p-1)/2$ ficam inalterados quando submetidos a uma rotação de um ângulo de $2\pi/p$ radianos. Estes são chamados p-ágonos estrelados regulares uma vez que são "estrelas" de p pontos onde cada ponto é o vértice de um ângulo de $(2k+1)\pi/p$ radianos, onde $0 \leq k < (p-1)/2$.

No caso $p = 5$, existem duas de tais figuras, mostradas na terceira linha da Figura 3.5. No caso $p = 13$ as seis figuras estão ilustradas na Figura 3.6.

Os restantes $p!/2p - (p-1)/2$ p-ágonos estrelados pertencem, naturalmente,

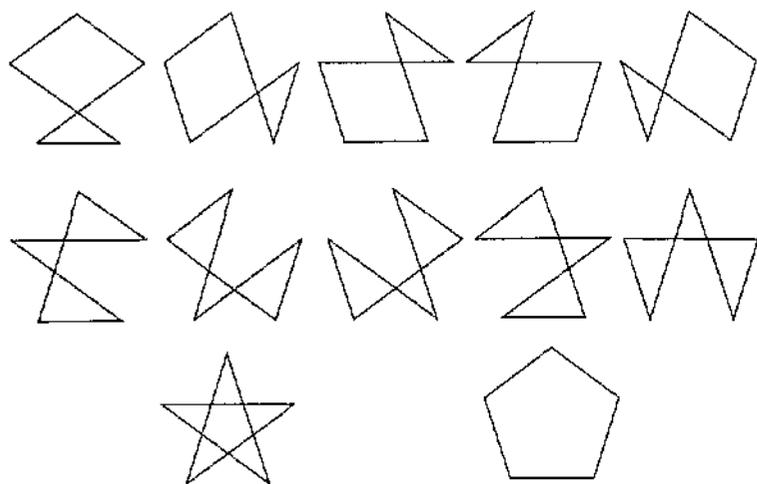



Figura 3.5

a conjuntos de p elementos onde os membros de cada conjunto podem ser obtidos de um único elemento por sucessivas rotações de $2\pi/p$ radianos. A observação de que existem p elementos em cada conjunto pode ser verificada como na demonstração do Pequeno Teorema de Fermat, onde nós mostramos que cada bracelete provém de p seqüências de contas. Quando $p = 5$, existem 2 de tais conjuntos que constituem as primeiras duas linhas da Figura 3.5. Desta forma, o número total de conjuntos é

$$\frac{\frac{p!}{2p} - \frac{p-1}{2}}{p} = \frac{(p-1)! - (p-1)}{2p}.$$

Como $2p|[(p-1)! - p + 1]$, então $p|[(p-1)! + 1]$. □

3.5 Problemas Propostos

1. Quantos estudantes uma turma precisa conter, no mínimo, para que pelo menos dois estudantes tirem notas iguais no exame final, dado que as notas variam de 0 a 10 e apenas uma casa decimal é utilizada quando necessário?

2. Suponha agora que as notas possíveis são conceitos A, B, C, D e F. Qual o número mínimo de estudantes para que pelo menos 5 tenham conceitos iguais?

3. Existem 25 milhões de linhas telefônicas em um determinado estado, identificadas por uma seqüência de 10 dígitos da forma NXX − NXX − XXXX, onde

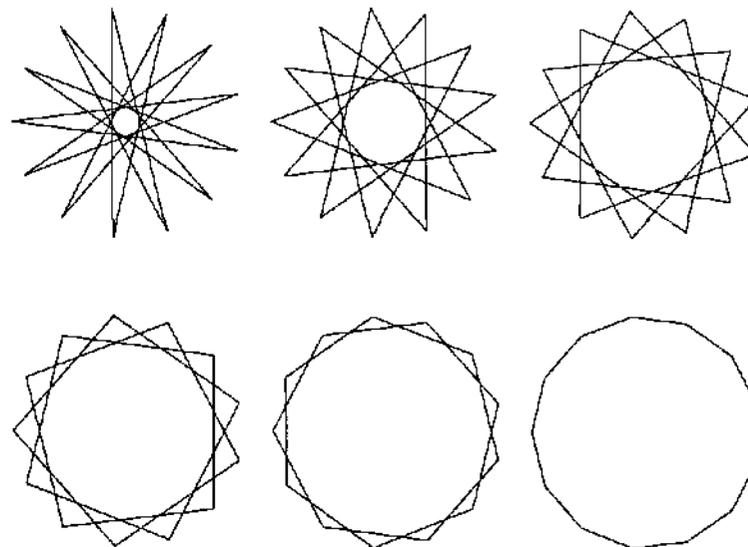



Figura 3.6

N é um dígito entre 2 e 9, inclusive, X é um dígito qualquer e os primeiros 3 dígitos constituem o código de DDD. Quantos códigos distintos de DDD o estado deve admitir para que a cada linha telefônica, corresponda uma seqüência de 10 dígitos distinta das demais?

4. Existem 83 casas em uma rua. As casas são numeradas com números entre 100 e 262 inclusive. Mostre que pelo menos 2 casas têm números consecutivos.

5. Quantas pessoas, no mínimo, devemos ter em um grupo para que possamos garantir a existência de pelo menos duas tendo nomes que começam com a mesma letra? (Considere um alfabeto com 26 letras).

6. Supondo que os números de RG sejam constituídos de 7 dígitos, quantas pessoas, no mínimo, devemos ter em uma cidade para que se tenha certeza da existência de pelo menos duas com os primeiros dois dígitos (da esquerda) iguais? (Admita que um RG possa ter "0" como dígito inicial.)

7. Uma escola possui 46 classes com uma média de 38 alunos por classe. O que se pode dizer a respeito do número de alunos na maior?

8. Um restaurante possui 62 mesas com um total de 314 cadeiras. É possível garantir a existência de pelo menos uma mesa com pelo menos 6 cadeiras?

9. Dados 12 livros de português, 14 de história, 9 de química e 7 de física, quantos livros devemos retirar (sem olhar) para que estejamos certos de termos

retirado 6 de uma mesma disciplina?

10. Mostrar que em um grupo de apenas 5 pessoas o resultado do Exemplo 3.17 não é necessariamente verdadeiro. (Sugestão: construir uma figura com os 5 pontos ligados por $C_5^2 = 10$ segmentos de reta, onde não exista nenhum triângulo tendo todos os lados de mesma cor)

11. Encontrar a maior subseqüência crescente e a maior subseqüência decrescente para cada uma das seqüências abaixo:
(a) 6, 4, 5, 3, 2;
(b) 8, 7, 9, 2, 3, 6, 10, 12, 15, 5;
(c) 5, 10, 2, 8, 3, 12, 14, 17, 9, 7;
verificando se elas estão em concordância com o Teorema 3.3. (As respostas não são únicas.)

12. Mostrar que 11 divide infinitos números da forma 363636...36.

Capítulo 4

Funções Aritméticas

4.1 Funções Aritméticas

Neste capítulo, introduzimos o conceito de funções aritméticas e apresentamos vários resultados sobre as funções aritméticas multiplicativas. Como será visto, para avaliarmos uma função multiplicativa é suficiente sabermos seu valor em potências de primos.

Embora neste trabalho estejamos abordando apenas aspectos elementares de algumas funções aritméticas multiplicativas, vale mencionar que este conceito é de fundamental importância em Teoria Algébricas de Números (produto de Dirichlet) e Teoria Analítica de Números (séries de Dirichlet).

Sobre números perfeitos, apresentamos uma caracterização dos perfeitos pares dada por Euclides e Euler. Introduzimos, também, os números de Fibonacci, apresentando apenas algumas propriedades desta importantíssima seqüência.

As Funções $\tau(n)$ e $\sigma(n)$

Definição 4.1 Chamamos *função aritmética* a uma função definida para todos os inteiros positivos.

A função ϕ de Euler é um exemplo de função aritmética. Definimos, a seguir, duas outras importantes funções aritméticas.

Definição 4.2 $\tau(n)$ é o número de divisores positivos de n. $\sigma(n)$ é a soma dos divisores positivos de n.

Com a notação de somatório podemos facilmente expressar estas definições da seguinte forma:

$$\tau(n) = \sum_{d|n} 1, \qquad \sigma(n) = \sum_{d|n} d.$$

O resultado abaixo nos dá uma fórmula para o cálculo de $\tau(n)$.

Proposição 4.1 *Se* $n = p_1^{a_1} p_2^{a_2} p_3^{a_3} \cdots p_r^{a_r}$, *então*

$$\tau(n) = (a_1+1)(a_2+1)\cdots(a_r+1).$$

Demonstração: Como todo número de forma p_1^t com $0 \le t \le a_1$ é um divisor de $p_1^{a_1}$, então o número de divisores de $p_1^{a_1}$ é (a_1+1). Caso n possua somente dois fatores primos distintos, i.e., $n = p_1^{a_1} p_2^{a_2}$, a Proposição 1.7, juntamente com o princípio multiplicativo nos garante $\tau(n) = (a_1+1)(a_2+1)$. O caso geral segue facilmente por indução. □

Exemplo 4.1 Como $12 = 2^2.3$ temos $\tau(12) = (2+1)\cdot(1+1) = 6$.

Definição 4.3 Uma *função multiplicativa* é uma função aritmética (não-nula) tal que $f(mn) = f(m)f(n)$ para todo par de inteiros positivos m e n relativamente primos.

Uma função aritmética para a qual $f(mn) = f(m)f(n)$ para quaisquer m e n é chamada completamente multiplicativa

O teorema seguinte nos permitirá concluir, imediatamente, que as funções $\tau(n)$ e $\sigma(n)$ são ambas multiplicativas.

Teorema 4.1 Se $f(n)$ é uma função multiplicativa então

$$F(n) = \sum_{d|n} f(d)$$

é também multiplicativa.

Demonstração: Devemos mostrar que $F(m\cdot n) = F(m)\cdot F(n)$ para m e n relativamente primos. Pela definição de $F(n)$ temos

$$F(m\cdot n) = \sum_{d|mn} f(d).$$

Como $(m,n) = 1$, a Proposição 1.7 nos diz que todo divisor de mn pode ser expresso, de modo único, como o produto de d_1 e d_2 onde $d_1|m, d_2|n$ e $(d_1, d_2) = 1$ e que para cada par de divisores d_1 de m e d_2 de n corresponde um único divisor $d = d_1 d_2$ de mn. Logo,

$$F(mn) = \sum_{d|mn} f(d) = \sum_{\substack{d_1|m \\ d_2|n}} f(d_1 d_2).$$

Mas, como f é, por hipótese, multiplicativa temos

$$F(mn) = \sum_{\substack{d_1|m \\ d_2|n}} f(d_1)f(d_2)$$

$$= \sum_{d_1|m} \sum_{d_2|n} f(d_1)f(d_2)$$

$$= \sum_{d_1|m} f(d_1) \sum_{d_2|m} f(d_2) = F(m)F(n).$$

Corolário 4.1 As funções $\tau(n)$ e $\sigma(n)$ são multiplicativas.

Demonstração: Como

$$\tau(n) = \sum_{d|n} 1, \quad \text{e} \quad \sigma(n) = \sum_{d|n} d,$$

o resultado segue, pois as funções $f(d) = 1$ e $f(d) = d$ são multiplicativas. □

Proposição 4.2 *Para* p *primo e* a *um inteiro positivo temos que*

$$\sigma(p^a) = \frac{p^{a+1}-1}{p-1} \qquad \text{e} \qquad \tau(p^a) = a+1.$$

Demonstração: Já vimos, na Proposição 4.1, que $\tau(p^a) = a+1$. Como $\sigma(p^a) = 1 + p + p^2 + \cdots + p^a$, a fórmula $\sigma(p^a) = (p^{a+1}-1)/(p-1)$ segue do fato de que para $x \neq 1$,

$$1 + x + x^2 + \cdots + x^n = \frac{x^{n+1}-1}{x-1}. \qquad \square$$

Proposição 4.3 *Se* $n = p_1^{a_1} p_2^{a_2} p_3^{a_3} \cdots p_r^{a_r}$, *então*

$$\sigma(n) = \prod_{i=1}^{r} \frac{p_i^{a_i+1}-1}{p_i-1} \quad \text{e} \quad \tau(n) = \prod_{i=1}^{r}(a_i+1).$$

Demonstração: Como $\tau(n)$ e $\sigma(n)$ são multiplicativas temos, pela Proposição 4.2,

$$\begin{aligned} \tau(n) &= \tau(p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}) \\ &= \tau(p_1^{a_1})\tau(p_2^{a_2})\cdots\tau(p_r^{a_r}) \\ &= (a_1+1)(a_2+1)\cdots(a_r+1) = \prod_{i=1}^{r}(a_i+1) \end{aligned}$$

e

$$\sigma(n) = \sigma(p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r})$$

$$\begin{aligned}
&= \sigma(p_1^{a_1})\sigma(p_2^{a_2})\cdots\sigma(p_r^{a_r}) \\
&= \frac{p_1^{a_1+1}-1}{p_1-1}\cdot\frac{p_2^{a_2+1}-1}{p_2-1}\cdots\frac{p_r^{a_r+1}-1}{p_r-1} \\
&= \prod_{i=1}^{r}\frac{p_i^{a_i+1}-1}{p_i-1}
\end{aligned}$$

A fórmula para $\sigma(n)$, dada por esta proposição, poderia também ser demonstrada através do princípio multiplicativo como fizemos para $\tau(n)$ na Proposição 4.1.

4.2 A Função ϕ de Euler

Voltamos, agora, nossa atenção para a função ϕ de Euler . Antes de demonstrarmos que esta função aritmética é também multiplicativa vamos demonstrar o seguinte teorema.

Teorema 4.2 *Para* p *primo e* a *um inteiro positivo temos*

$$\phi(p^a) = p^a - p^{a-1}.$$

Demonstração: Pela definição de $\phi(n)$ sabemos que $\phi(p^a)$ é o número de inteiros positivos não-superiores a p^a e relativamente primos com p^a. Mas os únicos números não primos com p^a e menores do que ou iguais a p^a são aqueles divisíveis por p. Como os múltiplos de p não-superiores a p^a são, em número, p^{a-1}, o resultado segue.

Exemplo 4.2 $\phi(4) = \phi(2^2) = 2^2 - 2^1 = 2$, $\phi(27) = \phi(3^3) = 3^3 - 3^2 = 18$.

Teorema 4.3 *A função* ϕ *de Euler é multiplicativa, isto é,* $\phi(mn) = \phi(m)\phi(n)$ *para* $(m,n) = 1$.

Demonstração: Vamos dispor os números de 1 até mn da seguinte forma:

$$\begin{array}{ccccc}
1 & m+1 & 2m+1 & \cdots & (n-1)m+1 \\
2 & m+2 & 2m+2 & \cdots & (n-1)m+2 \\
3 & m+3 & 2m+3 & \cdots & (n-1)m+3 \\
 & & & \vdots & \\
m & 2m & 3m & \cdots & nm
\end{array}$$

Se na linha r, onde estão os termos $r, m+r, 2m+r, \ldots, (n-1)m+r$, tivermos $(m,r) = d > 1$, então nenhum termo nesta linha será primo com mn, uma vez que estes termos, sendo da forma $km+r, 0 \le k \le n-1$, são

todos divisíveis por d que é o máximo divisor comum de m e r. Logo, para encontrarmos os inteiros desta tabela que são primos com mn, devemos olhar na linha r somente se $(m,r) = 1$. Portanto temos $\phi(m)$ linhas onde todos os elementos são primos com m.

Devemos, pois, procurar em cada uma dessas $\phi(m)$ linhas, quantos elementos são primos com n, uma vez que todos são primos com m. Como $(m,n) = 1$ os elementos $r, m+r, 2m+r, \ldots, (n-1)m+r$ formam um sistema completo de resíduos módulo n. Logo, cada uma destas linhas possui $\phi(n)$ elementos primos com n e, portanto, como eles são primos com m, eles são primos com mn. Isto nos garante que $\phi(mn) = \phi(m)\phi(n)$. □

Teorema 4.4 *Para* $n = p_1^{a_1}p_2^{a_2}p_3^{a_3}\ldots p_r^{a_r}$, *temos*

$$\phi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_r}\right).$$

Demonstração: Pelo Teorema 4.2 temos

$$\phi(p_i^{a_i}) = p_i^{a_i} - p_i^{a_i-1} = p_i^{a_i}(1-\frac{1}{p_i}).$$

Portanto o teorema anterior nos garante que

$$\begin{aligned}
\phi(p_1^{a_1}p_2^{a_2}\cdots p_r^{a_r}) &= p_1^{a_1}(1-\frac{1}{p_1})p_2^{a_2}(1-\frac{1}{p_2})\cdots p_r^{a_r}(1-\frac{1}{p_r}) \\
&= p_1^{a_1}p_2^{a_2}\cdots p_r^{a_r}(1-\frac{1}{p_1})(1-\frac{1}{p_2})\cdots(1-\frac{1}{p_r}) \\
&= n(1-\frac{1}{p_1})(1-\frac{1}{p_2})\cdots(1-\frac{1}{p_r}).
\end{aligned}$$ □

Antes de demonstrarmos o próximo teorema, apresentamos um caso especial do mesmo para ilustrarmos a idéia usada na demonstração. Consideramos $n = 20$. Os divisores de 20 são: 1, 2, 4, 5, 10 e 20. É claro que o máximo divisor comum de qualquer número $m, 1 \le m \le 20$ e 20, é um dos divisores de 20. Vamos separar os números de 1 a 20 em conjuntos A_i, onde i é um dos divisores de 20, colocando em A_i todos os m's, tais que $(m, 20) = i$. Desta forma temos

$$\begin{aligned}
A_1 &= \{1,3,7,9,11,13,17,19\}, \\
A_2 &= \{2,6,14,18\}, \\
A_4 &= \{4,8,12,16\}, \\
A_5 &= \{5,15\},
\end{aligned}$$

$$A_{10} = \{10\},$$
$$A_{20} = \{20\}.$$

Estes conjuntos são, obviamente, disjuntos e a união deles é o conjunto $\{1, 2, 3, \ldots, 20\}$. Na tabela abaixo temos o número de elementos para cada A_i.

Conjunto A_i	Número de elementos em A_i
A_1	$8 = \phi(20) = \phi(20/1)$
A_2	$4 = \phi(10) = \phi(20/2)$
A_4	$4 = \phi(5) = \phi(20/4)$
A_5	$2 = \phi(4) = \phi(20/5)$
A_{10}	$1 = \phi(2) = \phi(20/10)$
A_{20}	$1 = \phi(1) = \phi(20/20)$

Observe que, se i é um divisor de 20, $20/i$ também é. Mostramos, pois, que

$$\sum_{d|20} \phi(d) = 20.$$

No teorema seguinte mostramos que este resultado vale em geral.

Teorema 4.5 *Para qualquer inteiro n temos,*

$$\sum_{d|n} \phi(d) = n.$$

Demonstração: Separamos o conjunto $\{1, 2, 3, \ldots, n\}$ em classes A_d, uma para cada divisor d de n. Na classe A_d colocamos todos os elementos m, onde $1 \leq m \leq n$, tais que $(m, n) = d$. Sabemos, pelo corolário da Proposição 1.4 que $(m, n) = d$ se, e somente se, $(m/d, n/d) = 1$. Como $m/d \leq n/d$, podemos concluir que m está em A_d se m/d for relativamente primo com n/d. Logo, em A_d temos exatamente $\phi(n/d)$ elementos. Como cada elemento m de $\{1, 2, \ldots, n\}$ se encontra em somente uma das classes A_d, temos que

$$\sum_{d|n} \phi(n/d) = n.$$

O fato de que para cada divisor d de $n, n/d$ é também um divisor de n, significa que quando d percorre o conjunto dos divisores de $n, n/d$ também percorre este mesmo conjunto. Portanto, $\sum_{d|n} \phi(d) = n$. □

4.3 A Função μ de Möbius

Definimos a seguir uma importante função aritmética que também é multiplicativa, a função μ de Möbius.

Definição 4.4 A *função μ de Möbius* é definida por,

$$\mu(1) = 1 \quad \text{e, para} \quad n = p_1^{a_1} p_2^{a_2} \ldots p_r^{a_r}$$
$$\mu(n) = (-1)^r \quad \text{se} \quad a_1 = a_2 = \ldots = a_r = 1$$
$$\mu(n) = 0 \quad \text{caso contrário}$$

Esta definição nos diz, portanto, que $\mu(n) = 0$ sempre que n for divisível pelo quadrado de algum primo.

Exemplo 4.3 $\mu(2) = -1$, $\mu(6) = \mu(2 \times 3) = (-1)^2$, $\mu(12) = 0$, $\mu(30) = (-1)^3 = -1$, pois $30 = 2 \times 3 \times 5$.

Teorema 4.6 *A função μ de Möbius é multiplicativa.*

Demonstração: Sejam m e n tais que $(m, n) = 1$. Se para algum primo $p, p^2|mn$, então $p^2|m$ ou $p^2|n$, uma vez que $(m, n) = 1$. Logo, em ambos os casos $\mu(mn) = \mu(m)\mu(n)$. Se nenhum deles é divisível pelo quadrado de nenhum primo, então $m = p_1p_2 \ldots p_r$ e $n = q_1q_2 \ldots q_s$ e, portanto, $mn = p_1p_2 \cdots p_rq_1q_2 \cdots q_s$. Logo,

$$\mu(mn) = (-1)^{r+s} = (-1)^r(-1)^s = \mu(m)\mu(n),$$

o que conclui a demonstração. □

Teorema 4.7

$$F(n) = \sum_{d|n} \mu(d) = \begin{cases} 1 & \text{se} \quad n = 1 \\ 0 & \text{se} \quad n > 1 \end{cases}$$

Demonstração: Sendo $\mu(d)$ multiplicativa, o Teorema 4.1 nos garante que $F(n)$ é multiplicativa. É, pois, suficiente avaliarmos $F(n)$ para $n = p^r$. Mas,

$$\begin{aligned} F(p^r) = \sum_{d|p^r} \mu(d) &= \mu(1) + \mu(p) + \mu(p^2) + \cdots + \mu(p^r) \\ &= 1 + \mu(p) = 1 - 1 = 0. \end{aligned}$$

Logo $F(n) = 0$ para todo $n > 1$ e como $F(1) = 1$ a demonstração está completa.

Uma outra maneira de demonstrarmos este resultado seria observar que na soma

$$\sum_{d|n} \mu(d)$$

os únicos termos que não são nulos vêm de $d = 1$ e dos divisores que são produtos de primos distintos, i.e.,

$$\begin{aligned}\sum_{d|n} \mu(d) = 1 + \mu(p_1) + \cdots + \mu(p_r) + \mu(p_1p_2) + \mu(p_1p_3) + \\ + \cdots + \mu(p_1p_r) + \cdots + \mu(p_1p_2\cdots p_r) \\ = 1 + \binom{r}{1}(-1) + \binom{r}{2}(-1)^2 + \cdots + \binom{r}{r}(-1)^r \\ = (1-1)^r = 0.\end{aligned}$$

onde, na última linha, foi usada a fórmula da expansão do binômio de Newton. □

4.4 A Função Maior Inteiro

Definimos, abaixo, a função "*maior inteiro*". Esta é uma importante função em Teoria dos Números que introduzimos aqui, embora não seja, pela nossa definição, uma função aritmética.

Definição 4.5. A função "*maior inteiro*" é a que associa a cada real x o maior inteiro menor do que ou igual a x. Denotamos este valor por $\lfloor x \rfloor$.

Exemplo: $\lfloor 2 \rfloor = 2$; $\lfloor 3,2 \rfloor = 3$; $\lfloor -5,1 \rfloor = -6$; $\lfloor 0,380 \rfloor = 0$.

No teorema seguinte temos algumas propriedades desta função.

Teorema 4.8 Para um número real x temos:

1. $\lfloor x + n \rfloor = \lfloor x \rfloor + n$, para todo inteiro n.
2. $\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1, x - 1 < \lfloor x \rfloor \leq x$, $0 \leq x - \lfloor x \rfloor < 1$.
3. Se $x \notin \mathbb{Z}$, então $\lfloor -x \rfloor = -\lfloor x \rfloor - 1$.
4. $\lfloor x \rfloor + \lfloor y \rfloor \leq \lfloor x + y \rfloor \leq \lfloor x \rfloor + \lfloor y \rfloor + 1$.
5. $\lfloor x \rfloor + \lfloor -x \rfloor = 0$ se x é um inteiro e -1 se $x \notin \mathbb{Z}$.
6. $\left\lfloor \frac{\lfloor x \rfloor}{m} \right\rfloor = \left\lfloor \frac{x}{m} \right\rfloor$ para m um inteiro positivo.
7. $\lfloor 2x \rfloor - 2\lfloor x \rfloor = \begin{cases} 1 \text{ se } \lfloor 2x \rfloor \text{ é ímpar} \\ 0 \text{ se } \lfloor 2x \rfloor \text{ é par.} \end{cases}$
8. Se n é um inteiro positivo, $\lfloor n/a \rfloor$ é o número de inteiros do conjunto $\{1, 2, 3, \ldots, n\}$ que são divisíveis por a.

Demonstração: As afirmações (1), (2) e (3) são conseqüências imediatas da definição de $\lfloor x \rfloor$.

(4) Sejam $x = n + \alpha$ e $y = m + \beta$ onde n e m são inteiros e $0 \leq \alpha < 1$, $0 \leq \beta < 1$. Logo,

$$\begin{aligned}\lfloor x \rfloor + \lfloor y \rfloor &= n + m \\ &= \lfloor n + m \rfloor \\ &\leq \lfloor n + \alpha + m + \beta \rfloor \\ &= \lfloor x + y \rfloor \\ &= n + m + \lfloor \alpha + \beta \rfloor \\ &\leq n + m + 1 \\ &= \lfloor x \rfloor + \lfloor y \rfloor + 1.\end{aligned}$$

(5) Sendo $x = n + \alpha$, temos $-x = -n - 1 + 1 - \alpha$. Logo,

$$\begin{aligned}\lfloor x \rfloor + \lfloor -x \rfloor &= n + \lfloor -n - 1 + 1 - \alpha \rfloor \\ &\overset{(1)}{=} n - n - 1 + \lfloor 1 - \alpha \rfloor = 0\end{aligned}$$

se $\alpha = 0$, e -1 se $\alpha > 0$.

(6) Seja $x = n + \alpha$, $0 \leq \alpha < 1$. Sabemos, pelo algoritmo da divisão, que existem q e r tais que $n = qm + r$, $0 \leq r \leq m - 1$. Portanto,

$$\left\lfloor \frac{x}{m} \right\rfloor = \left\lfloor \frac{qm + r + \alpha}{m} \right\rfloor = \left\lfloor q + \frac{r + \alpha}{m} \right\rfloor = q$$

pois $0 \leq r + \alpha < m$, uma vez que $0 \leq \alpha < 1$ e $0 \leq r \leq m - 1$. Mas,

$$\left\lfloor \frac{\lfloor x \rfloor}{m} \right\rfloor = \left\lfloor \frac{n}{m} \right\rfloor = \left\lfloor \frac{qm + r}{m} \right\rfloor = \left\lfloor q + \frac{r}{m} \right\rfloor = q$$

o que prova (6).

(7) Se $x = n + \alpha$, $0 \leq \alpha < 1, \lfloor x \rfloor = n$. Se $0 \leq \alpha < 1/2$, então $2\alpha < 1$ e $\lfloor 2x \rfloor = \lfloor 2n + 2\alpha \rfloor = 2n$ é par, o que implica $\lfloor 2x \rfloor - 2\lfloor x \rfloor = 2n - 2n = 0$. Se $1/2 \leq \alpha < 1$, $1 \leq 2\alpha < 2$ e $\lfloor 2x \rfloor = \lfloor 2n + 2\alpha \rfloor = 2n + 1$ é impar e $\lfloor 2x \rfloor - 2\lfloor x \rfloor = 2n + 1 - 2n = 1$.

A demonstração de (8) está entre os problemas resolvidos no final deste capítulo. □

Conhecida esta função $\lfloor x \rfloor$, o Teorema 4.7 pode ser, agora, enunciado como:

$$\sum_{d|n} \mu(d) = \left\lfloor \frac{1}{n} \right\rfloor$$

Utilizando propriedades desta função "Maior Inteiro" apresentamos dois teoremas fundamentais. Um deles tem como corolário o fato de $\frac{n!}{k!(n-k)!}$ ser um inteiro para todos os naturais n e k com $k \leq n$.

Teorema 4.9 *Seja n um número natural e p um primo. Então o expoente da maior potência de p que divide $n!$ é dado por:*

$$N = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots \tag{4.1}$$

Demonstração: A série em (4.1) continua enquanto $p^\alpha \leq n$. Se h_α denota o número de termos na seqüência 1, 2, 3,..., n que são divisíveis por p^α, então o expoente N é, claramente, dado por $h_1 + h_2 + h_3 + \cdots$.

Os naturais $\leq n$ que são divisíveis por p^α são

$$1 \cdot p^\alpha, 2 \cdot p^\alpha, 3 \cdot p^\alpha, \ldots, \left\lfloor \frac{n}{p^\alpha} \right\rfloor . p^\alpha.$$

Desta forma temos que $h_\alpha = \left\lfloor \frac{n}{p^\alpha} \right\rfloor$ o que concluiu a prova do teorema. □

Observamos que, pelo Teorema 4.8(6), temos

$$h_{\alpha+1} = \left\lfloor \frac{h_\alpha}{p} \right\rfloor.$$

Isto nos diz que podemos determinar os números h_α dividindo, sucessivamente, por p e não por potências de p. Isto fornece uma maneira mais rápida de se determinar N.

Exemplo 4.4 Se $n = 19$ e $p = 2$ temos

$$\left\lfloor \frac{19}{2} \right\rfloor = 9\,;\; \left\lfloor \frac{9}{2} \right\rfloor = 4\,;\; \left\lfloor \frac{4}{2} \right\rfloor = 2\,;\; \left\lfloor \frac{2}{2} \right\rfloor = 1$$

Logo $N = 9 + 4 + 2 + 1 = 16$.

Teorema 4.10. *Se $n, n_1, n_2, \ldots, n_s$ são números naturais tais que*

$$n = n_1 + n_2 + \cdots + n_s$$

então o quociente

$$\frac{n!}{n_1! n_2! \ldots n_s!} \tag{4.2}$$

é um inteiro.

Demonstração: Seja m um número natural. Da relação

$$\frac{n}{m} = \frac{n_1}{m} + \frac{n_2}{m} + \cdots + \frac{n_s}{m}$$

obtemos, pelo Teorema 4.8(4), a desigualdade

$$\left\lfloor \frac{n}{m} \right\rfloor \geq \left\lfloor \frac{n_1}{m} \right\rfloor + \left\lfloor \frac{n_2}{m} \right\rfloor + \cdots + \left\lfloor \frac{n_s}{m} \right\rfloor. \tag{4.3}$$

Seja p um fator primo de $n!$ e substitua m, na desigualdade (4.3), sucessivamente por $p, p^2, p^3, \ldots$.

Adicionando-se as desigualdades assim obtidas temos

$$\sum_{i \geq 1} \left\lfloor \frac{n}{p^i} \right\rfloor \geq \sum_{i \geq 1} \left\lfloor \frac{n_1}{p^i} \right\rfloor + \sum_{i \geq 1} \left\lfloor \frac{n_2}{p^i} \right\rfloor + \cdots + \sum_{i \geq 1} \left\lfloor \frac{n_s}{p^i} \right\rfloor.$$

Pelo Teorema 4.9 a soma do lado esquerdo desta desigualdade é o expoente da maior potência de p que divide $n!$ e, pela mesma razão, a j-ésima soma do lado direito é o expoente da maior potência de p que divide $n_j!$.

Desta última desigualdade, concluímos que a maior potência de p que divide o denominador de (4.2) também divide o numerador. Portanto o número (4.2) é um inteiro.

Na seção seguinte fornecemos um resultado que relaciona as funções ϕ de Euler e μ de Möbius .

4.5 Uma Relação Entre as Funções ϕ e μ

Teorema 4.11 *Para todo inteiro $n \geq 1$, temos*

$$\phi(n) = \sum_{d|n} \mu(d) \frac{n}{d}.$$

Demonstração: Se $k \in \{1,2,3,\dots,n\}$, então $\lfloor 1/(n,k) \rfloor = 1$ se $(n,k) = 1$ e 0 se $(n,k) > 1$. Logo a função $\phi(n)$ pode ser expressa como

$$\phi(n) = \sum_{k=1}^{n} \left\lfloor \frac{1}{(n,k)} \right\rfloor.$$

Se nesta equação usarmos o fato de que

$$\sum_{d|n} \mu(d) = \left\lfloor \frac{1}{n} \right\rfloor$$

teremos,

$$\phi(n) = \sum_{k=1}^{n} \sum_{d|(n,k)} \mu(d).$$

Mas, se $d|(n,k)$ então $d|n$ e $d|k$, o que nos permite escrever a última soma como

$$\phi(n) = \sum_{k=1}^{n} \sum_{\substack{d|n \\ d|k}} \mu(d).$$

Nesta soma, para cada divisor d de n, devemos somar somente para os k que são múltiplos de d. Sabemos que $k = qd$, $1 \le k \le n$ se, e somente se, $1 \le q \le n/d$. Logo,

$$\begin{aligned} \phi(n) &= \sum_{d|n} \sum_{q=1}^{n/d} \mu(d) \\ &= \sum_{d|n} \mu(d) \sum_{q=1}^{n/d} 1 = \sum_{d|n} \mu(d) \frac{n}{d}. \end{aligned}$$

Nos Teoremas 4.5 e 4.11 provamos dois resultados relacionados com a função $\phi(n)$,

$$n = \sum_{d|n} \phi(d) \qquad \text{e} \qquad \phi(n) = \sum_{d|n} \mu(d) \frac{n}{d}.$$

Estas duas fórmulas representam um caso especial de um importante teorema sobre a função de Möbius, conhecido como fórmula de Inversão de Möbius, que apresentamos a seguir.

Teorema 4.12 (Fórmula de Inversão de Möbius) *Se duas funções aritméticas $f(n)$ e $g(n)$ satisfazem uma das duas condições*

$$f(n) = \sum_{d|n} g(d), \quad g(n) = \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right)$$

para todo n, então elas satisfazem as duas condições.

Demonstração: Supomos que

$$f(n) = \sum_{d|n} g(d),$$

nestas condições temos:

$$\begin{aligned} \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right) &= \sum_{dd'=n} \mu(d) f(d') \\ &= \sum_{dd'=n} \mu(d) \sum_{m|d'} g(m) \\ &= \sum_{dmh=n} \mu(d) g(m) \\ &= \sum_{mh'=n} g(m) \sum_{d|h'} \mu(d). \end{aligned}$$

Pelo Teorema 4.7 a soma $\sum_{d|h'} \mu(d)$ é igual a zero para $h' > 1$ e igual a 1 para $h' = 1$. Logo

$$\sum_{d|n} \mu(d) f\left(\frac{n}{d}\right) = g(n).$$

Reciprocamente, suponhamos

$$g(n) = \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right).$$

Então

$$\begin{aligned} \sum_{d|n} g(d) &= \sum_{d|n} \sum_{d'|d} \mu(d') f\left(\frac{d}{d'}\right) \\ &= \sum_{d'mh=n} \mu(d') f(m) \end{aligned}$$

$$= \sum_{mh'=n} f(m) \sum_{d'|h'} \mu(d')$$

Novamente, pelo Teorema 4.7, vemos que a soma

$$\sum_{d'|h'} \mu(d')$$

é igual a zero para $h' > 1$ e igual a 1 para $h' = 1$. Logo, $\sum_{d|n} g(d) = f(n)$. □

Como, pelo Teorema 4.5,

$$n = \sum_{d|n} \phi(d)$$

e as funções $f(n) = n$ e $g(n) = \phi(n)$ são ambas multiplicativas, o Teorema 4.11 é consequência imediata do Teorema 4.12.

4.6 Números Perfeitos

Definição 4.6 Dizemos que um número n é *perfeito* se ele for igual à soma de seus divisores próprios, i.e., dos divisores positivos menores do que n.

Utilizando-se da função $\sigma(n)$, um número é perfeito se $\sigma(n) = 2n$. Como a soma dos divisores próprios de 6 que são 1, 2 e 3 é 6, 6 é um número perfeito. O número 28 também é perfeito $(28 = 1+2+4+7+14)$. Não se conhece nenhum número perfeito ímpar e não temos nenhuma prova a respeito da existência ou não de tais números.

Até o presente momento são conhecidos somente 31 números perfeitos e não se sabe se a lista de tais números é finita ou não.

No teorema seguinte fornecemos um resultado cuja primeira parte já era conhecida por Euclides.

Teorema 4.13 (Euclides-Euler) *Se* $p = 2^{n+1}-1$ *for primo, então* $m = p(p+1)/2$ *é um número perfeito par, e se* m *for um número perfeito par, então* $m = 2^n(2^{n+1}-1)$*, onde* $2^{n+1}-1 = p$ *é um primo.*

Demonstração: Se $p = 2^{n+1} - 1$ é primo, então $2^n = (p+1)/2$. Logo, se tomarmos $m = 2^n p$ teremos, pela Proposição 4.3

$$\begin{aligned} c\sigma(m) &= \sigma(2^n p) = \sigma(2^n)\sigma(p) \\ &= \frac{(2^{n+1}-1)}{(2-1)}(p+1) = (2^{n+1}-1)(p+1) = p(p+1) = 2m. \end{aligned}$$

O que significa que m é perfeito.

Agora, se m é um número perfeito par, então $m = 2^n m_1$, onde m_1 é ímpar e $n > 0$. Como σ é multiplicativa,

$$\sigma(m) = \sigma(2^n)\sigma(m_1) = (2^{n+1}-1)\sigma(m_1).$$

Sendo m perfeito, $\sigma(m) = 2m = 2^{n+1}m_1$. Logo,

$$(2^{n+1}-1)\sigma(m_1) = 2^{n+1}m_1. \tag{4.4}$$

Sabemos que $(2^{n+1}-1, 2^{n+1}) = 1$, portanto se $d = (m_1, \sigma(m_1))$ temos que $(m_1/d, \sigma(m_1)/d) = 1$ e dividindo-se os dois membros da última equação por d obtemos

$$(2^{n+1}-1)\frac{\sigma(m_1)}{d} = 2^{n+1}\frac{m_1}{d},$$

o que nos permite concluir que

$$(2^{n+1}-1) | \frac{m_1}{d} \qquad \text{e} \qquad \frac{m_1}{d} | (2^{n+1}-1),$$

ou seja, que $m_1 = d(2^{n+1}-1)$. Logo, levando-se este valor de m_1 em (4.4) obtemos $\sigma(m_1) = 2^{n+1}d$.

Provamos, agora, que $d = 1$. Se d fosse diferente de 1, m_1 teria pelo menos os divisores $d, m_1, (2^{n+1}-1)$ e 1. E portanto,

$$\begin{aligned} c\sigma(m_1) &\geq m_1 + 2^{n+1} - 1 + 1 + d \\ &= d(2^{n+1}-1) + 2^{n+1} + d \\ &= d2^{n+1} - d + 2^{n+1} + d \\ &= (d+1)2^{n+1} > 2^{n+1}d = \sigma(m_1) \end{aligned}$$

o que é absurdo. Logo $d = 1$, $m_1 = 2^{n+1} - 1$ e $m = 2^n m_1 = 2^n(2^{n+1}-1)$. Precisamos provar que $m_1 = 2^{n+1} - 1$ é primo. Mas,

$$\begin{aligned} \sigma(m) &= \sigma(2^n)\sigma(m_1) \\ &= (2^{n+1}-1)(1 + m_1 + \sum_{\substack{1<h<m_1 \\ h|m_1}} h) \\ &\geq (2^{n+1}-1)(2^{n+1}-1+1) = 2m. \end{aligned}$$

Nesta desigualdade teremos a igualdade somente no caso em que a soma dos divisores h de m com $1 < h < m_1$ for nula. Como $\sigma(m) = 2m$ esta soma tem que ser nula, o que implica ser m_1 primo. □

4.7 Recorrência e Números de Fibonacci

Com o objetivo específico de definir e estudar algumas propriedades interessantes da seqüência de Fibonacci, vamos introduzir um tipo especial de função aritmética.

Para a, b, x_0 e x_1 números quaisquer definimos $f(0) = x_0$, $f(1) = x_1$ e $f(n+1) = af(n) + bf(n-1)$, $\forall n \geq 1$.

Pode-se mostrar que isto determina $f(n)$ de maneira única, dependendo somente de x_0, x_1, a e b.

Para facilitar a notação escrevemos $x_n = f(n)$. Com esta notação $f(n+1) = af(n) + bf(n-1)$ se escreve

$$x_{n+1} = ax_n + bx_{n-1}. \tag{4.5}$$

A esta relação chamamos recorrência.

Definição 4.7 Chamamos *seqüência de Fibonacci* ou, simplesmente, "números de Fibonacci" à sequência $F_0 = 0, F_1 = 1, \ldots, F_n, \ldots$, onde $F_{n+1} = F_n + F_{n-1}$.

É claro que esta seqüência é um caso especial da recorrência (4.5), onde tomamos $x_0 = 0$ e $x_1 = a = b = 1$.

Utilizando-se da relação (4.5), podemos encontrar x_n para qualquer n, mas com a desvantagem de termos que gerar os termos intermediários x_s para $s < n$. Seria, pois, vantajoso se pudéssemos obter uma fórmula que nos permitisse encontrar diretamente x_n em função de x_0, x_1, a e b. Isto, embora nem sempre possível, pode ser feito para a recorrência (4.5).

A equação (4.5) pode ser reescrita como

$$x_{n+1} - kx_n = (a-k)(x_n - kx_{n-1}) + (b + ak - k^2)x_{n-1}.$$

Se denotarmos as raízes de $k^2 - ak - b = 0$ por k_1 e k_2 teremos que $k_1 + k_2 = a$ e

$$x_{n+1} - k_1x_n = k_2(x_n - k_1x_{n-1})$$
$$x_{n+1} - k_2x_n = k_1(x_n - k_2x_{n-1}).$$

Por iterações sucessivas destas duas equações temos:

$$x_{n+1} - k_1x_n = k_2^n(x_1 - k_1x_0)$$
$$x_{n+1} - k_2x_n = k_1^n(x_1 - k_2x_0).$$

Subtração membro a membro nos dá:

$$(k_2 - k_1)x_n = (x_1 - k_1x_0)k_2^n - (x_1 - k_2x_0)k_1^n.$$

Neste caso se $k_1 \neq k_2$ temos:

$$x_n = \frac{(x_1 - k_1x_0)k_2^n - (x_1 - k_2x_0)k_1^n}{k_2 - k_1} \tag{4.6}$$

Portanto, esta última equação nos fornece a fórmula desejada no caso de raízes distintas k_1 e k_2.

Vamos considerar, agora, o caso em que $k^2 - ak - b = 0$ possui duas raízes iguais. Neste caso é óbvio que $a = 2k$ e $b = -k^2$. A recorrência (4.5) pode, portanto, ser escrita na forma:

$$x_{n+1} = 2kx_n - k^2x_{n-1}.$$

Por aplicações sucessivas desta fórmula podemos obter

$$x_2 = 2kx_1 - k^2x_0$$
$$x_3 = 2kx_2 - k^2x_1 = 3k^2x_1 - 2k^3x_0$$
$$x_4 = 2kx_3 - k^2x_2 = 4k^3x_1 - 3k^4x_0$$
$$x_5 = 2kx_4 - k^2x_3 = 5k^4x_1 - 4k^5x_0.$$

Uma cuidadosa observação da seqüência acima nos sugere a seguinte conjectura:

$$x_n = nk^{n-1}x_1 - (n-1)k^nx_0 \tag{4.7}$$

a qual pode ser demonstrada por indução. O caso $n = 1$ é óbvio. Vamos supor que (4.7) seja verdadeira para todo m menor do que ou igual a n. Logo

$$\begin{aligned} x_{n+1} &= 2kx_n - k^2x_{n-1} \\ &= 2k(nk^{n-1}x_1 - (n-1)k^nx_0) - k^2((n-1)k^{n-2}x_1 - (n-2)k^{n-1}x_0) \\ &= (n+1)k^nx_1 - nk^{n+1}x_0. \end{aligned}$$

o que prova a validade de (4.7) $\forall n, n \geq 1$.

Podemos, agora, obter uma fórmula explícita que nos forneça para cada n o enésimo número de Fibonacci F_n. Como, no caso da sequência de Fibonacci, $x_0 = 0$ e $x_1 = a = b = 1$, as raízes k_1 e k_2 de $k^2 - k - 1 = 0$ são

$$k_1 = \frac{(1-\sqrt{5})}{2} \quad \text{e} \quad k_2 = \frac{(1+\sqrt{5})}{2}.$$

e, portanto, de (4.6) temos:

$$F_n = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right) \tag{4.8}$$

Fazendo-se uso desta fórmula é possível provar várias outras propriedades que são satisfeitas pelos números de Fibonacci. Lembramos ao leitor que algumas relações já foram introduzidas nos exercícios do primeiro capítulo. Nos problemas resolvidos que apresentamos a seguir mostramos, dentre outras propriedades, que o máximo divisor comum de dois números de Fibonacci é, também, um número de Fibonacci.

4.8 Problemas Resolvidos

Problema 4.1 Mostrar que se $m|n$ então $F_m|F_n$, onde F_n é o n-ésimo número de Fibonacci.

Solução. Considerando $\alpha = \dfrac{1+\sqrt{5}}{2}$ e $\beta = \dfrac{1-\sqrt{5}}{2}$ temos, por (4.8), que $F_n = (\alpha^n - \beta^n)/\sqrt{5}$. Logo, como $m|n$ temos que $n = km$ e a identidade

$$\begin{aligned} F_n = \frac{\alpha^n-\beta^n}{\sqrt{5}} &= \frac{(\alpha^m)^k-(\beta^m)^k}{\sqrt{5}} \\ &= \left(\frac{\alpha^m-\beta^m}{\sqrt{5}}\right)((\alpha^m)^{k-1}+(\alpha^m)^{k-2}(\beta^m)+\cdots+ \\ &\qquad \alpha^m(\beta^m)^{k-2}+(\beta^m)^{k-1}) \\ &= F_m((\alpha^m)^{k-1}+\cdots+(\beta^m)^{k-1}) \end{aligned}$$

nos permite concluir que $F_m|F_n$.

Problema 4.2 Mostrar que os números de Fibonacci satisfazem

$$F_{m+n} = F_{m-1}F_n + F_mF_{n+1}. \tag{4.9}$$

Solução. Por indução em n. Para $n = 1$ temos:

$$F_{m+1} = F_{m-1}F_1 + F_mF_2 = F_{m-1} + F_m.$$

Supondo válida para todo $n \leq k$ temos

$$\begin{aligned} F_{m+k} &= F_{m-1}F_k + F_mF_{k+1} \\ F_{m+(k-1)} &= F_{m-1}F_{k-1} + F_mF_k \end{aligned}$$

as quais somadas, membro a membro, nos fornecem

$$F_{m+k} + F_{m+(k-1)} = F_{m-1}(F_k + F_{k-1}) + F_m(F_{k+1} + F_k)$$

isto é, $F_{m+(k+1)} = F_{m-1}F_{k+1} + F_mF_{k+2}$, o que conclui a prova por indução.

Observamos que a identidade (4.9) permite provar, por indução, o resultado já mostrado no Problema 4.1.

Problema 4.3 Mostrar que se $m = nq + r$, então $(F_m, F_n) = (F_n, F_r)$.

Solução. Pela identidade (4.9) temos $(F_m, F_n) = (F_{nq+r}, F_n) = (F_{nq-1}F_r + F_{nq}F_{r+1}, F_n)$. Como $F_n|F_{nq}$ e para $b|c$, $(a+c, b) = (a, b)$ (veja exercício 34 do cap. 1) segue que: $(F_m, F_n) = (F_{nq-1}F_r + F_{nq}F_{r+1}, F_n) = (F_{nq-1}F_r, F_n)$.

Mostramos, a seguir, que $(F_{nq-1}, F_n) = 1$. Seja $d = (F_{nq-1}, F_n)$. Como $d|F_n$ e $F_n|F_{nq}$ temos que $d|F_{nq}$ e $d|F_{nq-1}$ o que implica $d = 1$, pois números consecutivos de Fibonacci são primos entre si (ver exercício 14 do cap. 1).

Logo, como $(a, c) = 1$ implica $(a, bc) = (a, b)$ temos, $(F_m, F_n) = (F_{nq-1}F_r, F_n) = (F_n, F_r)$.

Problema 4.4 Mostrar que $(F_m, F_n) = F_{(m,n)}$.

Solução. Calculamos o máximo divisor comum de m e n pelo processo das divisões sucessivas descrito no Teorema 1.8.

Supondo $m > n$, temos:

$$\begin{aligned} m &= nq_1 + r_1, 0 < r_1 < n \\ n &= r_1q_2 + r_2, 0 < r_2 < r_1 \\ r_1 &= r_2q_3 + r_3, 0 < r_3 < r_2 \\ &\vdots \\ r_{n-2} &= r_{n-1}q_n + r_n, 0 < r_n < r_{n-1} \\ r_{n-1} &= r_nq_{n+1} + 0 \end{aligned}$$

Aplicamos o resultado do Problema 4.3 a cada uma das igualdades acima, obtendo $(F_m, F_n) = (F_n, F_{r_1}) = (F_{r_1}, F_{r_2}) = \cdots = (F_{r_{n-1}}, F_{r_n})$ Como $r_n|r_{n-1}$ temos $F_{r_n}|F_{r_{n-1}}$, donde concluímos que $(F_{r_{n-1}}, F_{r_n}) = F_{r_n} = F_{(m,n)}$ uma vez que r_n é o último resto não-nulo na seqüência de divisões acima.

Observamos que o que acabamos de provar implica que $m|n$ caso $F_m|F_n$, pois se $F_m|F_n$ então, $(F_m, F_n) = F_m$ e como $(F_m, F_n) = F_{(m,n)}$ concluímos que $m = (m, n)$, isto é, $m|n$.

Problema 4.5 Mostrar que $\phi(nm) = n\phi(m)$ se todo primo que divide n divide m.

Solução. Como todo fator primo de n divide m temos:

$$\begin{aligned} n &= p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_s^{\alpha_s} \\ m &= (p_1^{\beta_1}p_2^{\beta_2}\cdots p_s^{\beta_s})(q_1^{t_1}q_2^{t_2}\cdots q_r^{t_r}). \end{aligned}$$

Logo

$$\begin{aligned}\phi(n\cdot m) &= n\cdot m\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_s}\right)\\ &\cdot\left(1-\frac{1}{q_1}\right)\left(1-\frac{1}{q_2}\right)\left(1-\frac{1}{q_r}\right)\\ &= n\cdot\phi(m)\end{aligned}$$

Problema 4.6 Mostrar que

$$\phi(mn)=\frac{P\phi(m)\phi(n)}{\phi(P)}$$

onde P é o produto dos primos comuns a m e n.

Solução. Considerando

$$\begin{aligned}n &= p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_s^{\alpha_s}q_1^{t_2}q_2^{t_2}\cdots q_r^{t_r}\\ m &= p_1^{\beta_1}p_2^{\beta_2}\cdots p_s^{\beta_s}Q_1^{\gamma_1}Q_2^{\gamma_2}\cdots Q_v^{\gamma_v}).\end{aligned}$$

então $P=p_1p_2\ldots p_s$, de onde temos:

$$\begin{aligned}\phi(m\cdot n) &= m\cdot\left[n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_s}\right)\cdot\right.\\ &\left.\left(1-\frac{1}{q_1}\right)\left(1-\frac{1}{q_2}\right)\cdots\left(1-\frac{1}{q_r}\right)\right]\left(1-\frac{1}{Q_1}\right)\cdots\left(1-\frac{1}{Q_v}\right)\\ &= m\phi(n)\left(1-\frac{1}{Q_1}\right)\left(1-\frac{1}{Q_2}\right)\cdots\left(1-\frac{1}{Q_v}\right)\\ &= \phi(n)\frac{m\left(1-\frac{1}{Q_1}\right)\left(1-\frac{1}{Q_2}\right)\cdots\left(1-\frac{1}{Q_v}\right)\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_s}\right)}{\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_s}\right)}\\ &= \frac{P\phi(n)\phi(m)}{P\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_s}\right)}\\ &= \frac{P\phi(m)\phi(m)}{\phi(P)}.\end{aligned}$$

Problema 4.7 Mostrar que se $(m,n)>1$, então $\phi(mn)>\phi(m)\phi(n)$.

Solução. Utilizamos o resultado provado no problema anterior. Sendo $(m,n)>1$ temos que $\frac{P}{\phi(P)}>1$ e, portanto,

$$\phi(m\cdot n)=\frac{P}{\phi(P)}\phi(m)\phi(n)>\phi(m)\phi(n).$$

Problema 4.8 Mostrar que a soma dos números menores que n e primos com n é igual a $\frac{n\phi(n)}{2}$.

Solução. Sejam $a_1,a_2,\ldots,a_{\phi(n)}$ os inteiros positivos menores que n e primos com n. Pelo fato de $(a,n)=1$ implicar $(n-a,n)=1$, podemos concluir que $n-a_1,n-a_2,n-a_{\phi(n)}$ são todos primos com n. Sendo todos menores do que n eles são, a menos da ordem, os números $a_1,a_2,\ldots,a_{\phi(n)}$. Logo se somarmos as duas colunas abaixo teremos como resultado duas vezes a soma S que estamos procurando

$$\begin{array}{ll} a_1 & n-a_1\\ a_2 & n-a_2\\ \vdots & \vdots\\ a_{\phi(n)} & n-a_{\phi(n)}\end{array}$$

$a_1+a_2+\cdots+a_{\phi(n)}+(n-a_1)+(n-a_2)+\cdots+(n-a_{\phi(n)})=n\phi(n)=2\cdot S$, o que conclui a demonstração.

Problema 4.9 Mostrar que $\lfloor\frac{n}{a}\rfloor$ é o número de inteiros do conjunto $\{1,2,\ldots,n\}$ que são divisíveis por a.

Solução. Destacamos esta propriedade apenas para chamar a atenção para o fato importante, embora elementar, de que o quociente na divisão do inteiro n por $a(a\neq 0)$ é igual a $\left\lfloor\frac{n}{a}\right\rfloor$, isto é,

$$n=\left\lfloor\frac{n}{a}\right\rfloor a+r,\ 0\leq r<a.$$

Problema 4.10 Mostrar que se m é um inteiro positivo, então

$$\sum_{n=1}^{m}\mu(n)\left\lfloor\frac{m}{n}\right\rfloor=1$$

Solução. Pelo Teorema 4.7 sabemos que

$$\sum_{d_1|1}\mu(d_1)+\sum_{d_2|2}\mu(d_2)+\cdots+\sum_{d_m|m}\mu(d_m)=1$$

Como 1 é divisor de cada inteiro do conjunto $1,2,\ldots,m$, $\mu(1)$ irá ocorrer m vezes na soma acima, 2, sendo divisor de $\left\lfloor\frac{m}{2}\right\rfloor$ destes inteiros $\mu(2)$ ocorrerá

$\left\lfloor \frac{m}{2} \right\rfloor$ vezes. Em geral, sendo d divisor de $\left\lfloor \frac{m}{d} \right\rfloor$ dos inteiros de 1 a $m, \mu(d)$ aparecerá $\left\lfloor \frac{m}{d} \right\rfloor$ vezes nesta soma. Logo

$$\sum_{n=1}^{m}\left(\sum_{d|n}\mu(d)\right) = \mu(1)\left\lfloor \frac{m}{1} \right\rfloor + \mu(2)\left\lfloor \frac{m}{2} \right\rfloor + \cdots + \mu(m)\left\lfloor \frac{m}{m} \right\rfloor$$

e

$$\sum_{n=1}^{m}\mu(n)\left\lfloor \frac{m}{n} \right\rfloor = 1.$$

4.9 Problemas Propostos

1. Avaliar $\tau(n), \sigma(n)$ e $\phi(n)$ para os seguintes valores de n: a) 10 b) 35 c) 200 d) 512 e) 10000 f) 1234.

2. Para quais valores de $m, \phi(m)$ é ímpar?

3. Para quais valores de $m, \phi(m)$ divide m?

4. Mostrar que se m e n são inteiros positivos tais que $m|n$, então $\phi(m)|\phi(n)$.

5. Refazer a demonstração do Teorema 4.3 para $m = 5$ e $n = 9$.

6. Mostrar que $\phi(m)$ é par se $m > 2$.

7. Mostrar que existem infinitos inteiros m para os quais $\phi(m)$ é um quadrado perfeito.

8. Mostrar que se f é multiplicativa, então $f(1) = 1$.

9. Mostrar que para qualquer inteiro positivo n

$$\prod_{i=0}^{3}\mu(n+i) = 0.$$

10. Mostrar que um inteiro p é um primo se, e somente se, $\sigma(p) = p + 1$.

11. Mostramos que as funções $\tau(n)$ e $\sigma(n)$ são multiplicativas. Mostrar que nenhuma delas é completamente multiplicativa.

12. Mostrar que para um inteiro fixo r, a função $h(n) = n^r$ é completamente multiplicativa.

13. Mostrar que as funções $F(n) = f(n)g(n)$ e $G(n) = f(n)/g(n)$ são multiplicativas sendo $f(n)$ e $g(n)$ multiplicativas com $g(n) \neq 0$.

14. Mostrar, através de um exemplo, que a função $F(n) = \sum_{d|n} f(d)$ nem sempre é completamente multiplicativa caso $f(d)$ seja.

15. Mostrar que para qualquer inteiro positivo $n > 1$ existem infinitos inteiros m tais que $\tau(m) = n$.

16. Encontrar o menor inteiro positivo m para o qual $\sigma(n) = 6$.

17. Encontrar o menor inteiro positivo m para o qual $\phi(n) = 6$.

18. Mostrar que $\prod_{d|n} d = n^{\tau(n)/2}$.

19. Mostrar que se f é multiplicativa, $m|n$ e $(m, n/m) = 1$, então $f(n/m) = f(n)/f(m)$.

20. Seja $h(n)$ o número de fatores primos distintos de n. Por exemplo $h(15) = h(21) = 2$ e $h(30) = 3$. Seja $q(n) = a^{h(n)}$ onde a está fixado. Mostrar que $q(n)$ é multiplicativa mas não é completamente multiplicativa.

21. Mostrar que existem infinitos inteiros m para os quais $10|\phi(m)$. (Sugestão $\phi(11) = 10$).

22. Mostrar que se n é um inteiro, então

$$\phi(2n) = \begin{cases} \phi(n) & \text{se } n \text{ é ímpar} \\ 2\phi(n) & \text{se } n \text{ é par.} \end{cases}$$

23. Mostrar que todo inteiro positivo pode ser escrito como soma de números de Fibonacci distintos e não-consecutivos.

Capítulo 5

Resíduos Quadráticos

5.1 Resíduos Quadráticos

Neste capítulo estaremos interessados no estudo de soluções para a congruência $x^2 \equiv a(\text{mod } m)$. No caso em que m é primo ímpar e $(a, m) = 1$, esta congruência, caso tenha solução, tem exatamente duas soluções incongruentes. Isto é o que provamos no teorema abaixo.

Teorema 5.1 *Para p um primo ímpar e a um inteiro não-divisível por p, a congruência*

$$x^2 \equiv a(\text{mod } p),$$

caso tenha solução, tem exatamente duas soluções incongruentes módulo p.

Demonstração: Caso esta congruência tenha uma solução x_1, claramente $-x_1$ também será solução, uma vez que $(-x_1)^2 = x_1^2 \equiv a(\text{mod } p)$. Devemos mostrar que estas soluções x_1 e $-x_1$ são incongruentes módulo p. Se $x_1 \equiv -x_1(\text{mod } p)$, então teríamos $2x_1 \equiv 0(\text{mod } p)$ e, como p é ímpar e $p \nmid x_1$ (pois $p \mid (x_1^2 - a)$ e $p \nmid a$), isto é impossível. Precisamos mostrar que só existem duas soluções incongruentes. Seja y uma solução de $x^2 \equiv a(\text{mod } p)$, i.e., $y^2 \equiv a(\text{mod } p)$. Como x_1 é solução temos $x_1^2 \equiv y^2 \equiv a(\text{mod } p)$ e, portanto, $x_1^2 - y^2 = (x_1 + y)(x_1 - y) \equiv 0(\text{mod } p)$. Logo, $p \mid (x_1 + y)$ ou $p \mid (x_1 - y)$, o que implica $y \equiv -x_1(\text{mod } p)$ ou $y \equiv x_1(\text{mod } p)$. Com isto mostramos que, caso exista uma solução, existem exatamente duas soluções incongruentes. □

Teorema 5.2 (Lagrange) *Seja $f(x) = c_n x^n + c_{n-1}x^{n-1} + \cdots + c_2x^2 + c_1x + c_0$ um polinômio com coeficientes inteiros tal que $(c_n, p) = 1$, onde p é primo. Nestas condições a congruência*

$$f(x) \equiv 0(\text{mod } p),$$

tem no máximo n soluções. É claro que quando $n > p$ a congruência acima não tem mais do que p soluções distintas módulo p.

Demonstração: A demonstração será feita por indução em n, o grau do polinômio $f(x)$. Para $n = 1$ temos a congruência linear

$$f(x) = c_1x + c_0 \equiv 0(\text{mod } p).$$

Como, por hipótese, $(c_1, p) = 1$, o Teorema 2.8 nos garante que $c_1x \equiv -c_0(\text{mod } p)$ tem exatamente uma solução. Logo, o resultado é válido para $n = 1$. Assumimos o resultado verdadeiro para todo polinômio de grau $n - 1$. A prova que apresentamos é por contradição. Vamos supor que a congruência $f(x) \equiv 0(\text{mod } p)$ tenha $n + 1$ soluções incongruentes módulo p. Sejam $x_0, x_1, x_2, \ldots, x_n$ estas $n + 1$ soluções. É fácil verificar que

$$\begin{aligned} f(x) - f(x_0) &= c_n(x^n - x_0^n) + c_{n-1}(x^{n-1} - x_0^{n-1}) + \cdots + c_1(x - x_0) \\ &= (x - x_0)h(x), \end{aligned}$$

uma vez que $(x^i - x_0^i)$ é divisível por $x - x_0$ para todo inteiro i, $i = 1, 2, \ldots, n$ e que $h(x)$ é um polinômio de grau $n - 1$ tendo c_n como coeficiente de x^{n-1}. Como $f(x_k) \equiv f(x_0)(\text{mod } p)$, temos

$$f(x_k) - f(x_0) = (x_k - x_0)h(x_k) \equiv 0(\text{mod } p).$$

Isto implica que, para $k \neq 0, h(x_k) \equiv 0(\text{mod } p)$ pois $x_k \not\equiv x_0(\text{mod } p)$ se $x_k \neq x_0$. Portanto a congruência $h(x) \equiv 0(\text{mod } p)$ possui n soluções incongruentes módulo p, o que contradiz nossa hipótese de indução, uma vez que $(c_n, p) = 1$ e $h(x)$ tem grau $n - 1$. Logo, $f(x)$ não pode ter mais do que n soluções incongruentes módulo p, o que conclui a demonstração. □

Teorema 5.3 *Seja $f(x) = c_nx^n + c_{n-1}x^{n-1} + \cdots + c_2x^2 + c_1x + c_0$ um polinômio de grau n com coeficientes inteiros. Se a congruência*

$$f(x) \equiv 0(\text{mod } p), \qquad (p \text{ primo})$$

tiver mais do que n soluções, então todo coeficiente de f é divisível por p.

Demonstração: Vamos supor que algum coeficiente não seja divisível por p. Seja j o maior índice para o qual c_j não é divisível por p. Neste caso,

$$c_jx^j + c_{j-1}x^{j-1} + \cdots + c_1x + c_0 \equiv 0(\text{mod } p).$$

Como esta congruência tem mais do que n soluções, pelo Teorema de Lagrange, p deve dividir c_j, o que é uma contradição. Isto conclui a demonstração. □

Teorema 5.4 *Para* p *primo todos os coeficientes do polinômio abaixo são divisíveis por* p. $f(x) = (x-1)(x-2)\dots(x-p+1) - x^{p-1} + 1$.

Demonstração: Seja $h(x) = (x-1)(x-2)\dots(x-(p-1))$. É claro que os números $1, 2, 3, \dots, p-1$ são raízes de $h(x)$ e portanto soluções de $h(x) \equiv 0 (\text{mod } p)$. Como estes números são relativamente primos com p, pelo Pequeno Teorema de Fermat, todos eles são soluções de $g(x) = x^{p-1} - 1 \equiv 0 (\text{mod } p)$. Logo, como $f(x) = h(x) - g(x)$ é um polinômio de grau $p-2$ e possui $p-1$ raízes, o teorema anterior nos garante que p divide todos os coeficientes de $f(x)$. □

Corolário 5.1 (Teorema de Wilson) Para todo primo p, temos

$$(p-1)! \equiv -1 (\text{mod } p).$$

Demonstração: No teorema acima o termo constante é $(p-1)! + 1$ e este, sendo divisível por p, nos garante o resultado desejado. □

Definição 5.1 Sejam a e m inteiros com $(a, m) = 1$. Dizemos que a é um *resíduo quadrático* módulo m se a congruência $x^2 \equiv a (\text{mod } m)$ tiver solução. Caso $x^2 \equiv a (\text{mod } m)$ não tenha nenhuma solução, dizemos que a não é um resíduo quadrático módulo m ou que a é um resíduo não-quadrático.

Como $3^2 \equiv 1 (\text{mod } 8)$, então 1 é um resíduo quadrático módulo 8. $4^2 \equiv 2 (\text{mod } 7)$ e portanto 2 é um resíduo quadrático módulo 7. Vamos considerar o primo 13 e achar todos os números que são resíduos quadráticos módulo 13. Para isto é suficiente considerarmos os quadrados dos números 1,2,3,...,12. Observe que estes números formam um sistema reduzido de resíduos módulo 13.

$$1^2 \equiv 1 (\text{mod } 13)$$
$$2^2 \equiv 4 (\text{mod } 13)$$
$$3^2 \equiv 9 (\text{mod } 13)$$
$$4^2 \equiv 3 (\text{mod } 13)$$
$$5^2 \equiv 12 (\text{mod } 13)$$
$$6^2 \equiv 10 (\text{mod } 13)$$
$$7^2 \equiv 10 (\text{mod } 13)$$
$$8^2 \equiv 12 (\text{mod } 13)$$
$$9^2 \equiv 3 (\text{mod } 13)$$

$$10^2 \equiv 9 (\text{mod } 13)$$
$$11^2 \equiv 4 (\text{mod } 13)$$
$$12^2 \equiv 1 (\text{mod } 13)$$

Na coluna da esquerda temos os quadrados dos números de 1 até 12 e na coluna da direita apenas os 6 números 1,3,4,9,10 e 12. Estes são todos os resíduos quadráticos módulo 13. Observe que estes números aparecem na metade superior da tabela acima e que eles estão repetidos na metade inferior. O fato de haver repetição a partir do 7^2 vem da congruência $(13-k)^2 \equiv k^2 (\text{mod } 13)$ que é de verificação imediata. No caso de um primo ímpar qualquer pode-se mostrar que, dentre os elementos $1, 2, \dots, p-1$, que constituem um sistema reduzido de resíduos módulo p, metade, i.e., $(p-1)/2$ são resíduos quadráticos e os $(p-1)/2$ restantes, não são. Este é o resultado provado no teorema seguinte.

Teorema 5.5 *Seja* p *um primo ímpar. Dentre os números* $1, 2, \dots, p-1$, $(p-1)/2$ *são resíduos quadráticos e* $(p-1)/2$ *não são.*

Primeira Demonstração: Vamos considerar, como fizemos no caso $p = 13$, os quadrados dos números de 1 a $p-1$. Como $1^2 \equiv 1 (\text{mod } p)$ sabemos pelo Teorema 5.1, que -1 também é solução de $x^2 \equiv 1 (\text{mod } p)$, mas $-1 \equiv p-1 (\text{mod } p)$. Logo, 1 e $p-1$ são as únicas soluções de $x^2 \equiv 1 (\text{mod } p)$. Tomamos, agora, 2^2 que será congruente a algum número k diferente de 1. Como $-2 \equiv p-2 (\text{mod } p)$, 2 e $p-2$ são as únicas soluções incongruentes de $x^2 \equiv k (\text{mod } p)$. É claro que se $p > 3$, k será igual a 4. Veja o caso de $p = 13$ descrito acima. Já temos, portanto, dois pares, $(1, p-1)$ e $(2, p-2)$, cada par sendo as duas únicas soluções de uma congruência do tipo $x^2 \equiv a (\text{mod } p)$. Procedendo desta maneira teremos, ao final, $(p-1)/2$ pares, cada um solução para uma dentre $(p-1)/2$ congruências $x^2 \equiv a_i (\text{mod } p)$ associados a exatamente $(p-1)/2$ dos números $1, 2, 3, \dots, p-1$. Os $(p-1)/2$ números a_i's são os $(p-1)/2$ resíduos quadráticos. Os restantes $(p-1)/2$ não são resíduos quadráticos.

Segunda Demonstração: Consideramos os quadrados dos números $1, 2, 3, \dots, (p-1)/2$, isto é,

$$1^2, 2^2, 3^2, \dots, \left(\frac{p-1}{2}\right)^2.$$

Vamos mostrar que estes quadrados são incongruentes módulo p. Sejam x e y tais que $1 \le x \le (p-1)/2$ e $1 \le y \le (p-1)/2$ e suponhamos que $x^2 \equiv y^2 (\text{mod } p)$. Logo, $x^2 - y^2 = (x+y)(x-y) \equiv 0 (\text{mod } p)$ e, portanto, $p | (x+y)(x-y)$. Mas $p \nmid (x+y)$ uma vez que $x + y < p$. Logo $p | (x-y)$ o que

implica $x \equiv y(\text{mod } p)$ e, portanto, $x = y$ (lembre-se que x e y são positivos e menores do que p). Desta forma, concluímos que os quadrados acima são todos incongruentes módulo p. É fácil a verificação de que quando k percorre o conjunto $\{1, 2, \ldots, (p-1)/2\}$, $p - k$ percorre o conjunto

$$\left\{\frac{p+1}{2}, \frac{p+3}{2}, \ldots, p-1\right\}.$$

Logo, como $(p-k)^2 \equiv k^2(\text{mod } p)$, concluímos que os resíduos quadráticos pertencem às classes de congruências que contém os quadrados

$$1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2.$$

Portanto $(p-1)/2$ é o número de resíduos quadráticos dentre os números $1, 2, \ldots, p-1$. Os outros $(p-1)/2$ não são resíduos quadráticos. □

No teorema seguinte mostramos um resultado que será importante no Capítulo 7 e no qual fazemos uso do Teorema de Wilson .

Teorema 5.6 *Para* p *primo, a congruência* $x^2 \equiv -1(\text{mod } p)$ *tem solução se, e somente se,* $p = 2$ *ou* $p \equiv 1(\text{mod } 4)$.

Demonstração: É claro que $x = 1$ nos fornece uma solução se $p = 2$. Vamos construir uma solução para o caso $p \equiv 1(\text{mod } 4)$.

Para p um primo ímpar podemos escrever o Teorema de Wilson da seguinte forma:

$$\left(1 \cdot 2 \cdot 3 \cdots j \cdots \frac{p-1}{2}\right)\left(\frac{p+1}{2} \cdots (p-j) \cdots (p-2)(p-1)\right) \equiv -1(\text{mod } p)$$

Observamos que o produto $(p-1)!$ está dividido em duas partes, cada uma com o mesmo número de fatores. Podemos reescrever este produto formando pares, uma vez que para cada fator j na primeira parte temos o fator $(p-j)$ na segunda. Logo, o Teorema de Wilson pode ser escrito como:

$$\prod_{j=1}^{(p-1)/2} j(p-j) \equiv -1 \ (\text{mod } p).$$

Como $j(p-j) \equiv -j^2(\text{mod } p)$ temos:

$$-1 \equiv \prod_{j=1}^{(p-1)/2} (-j^2) \equiv (-1)^{(p-1)/2}\left(\prod_{j=1}^{(p-1)/2} j\right)^2 (\text{mod } p).$$

Mas sendo $p \equiv 1(\text{mod } 4)$, $(p-1)/2$ é par e, portanto,

$$x = \prod_{j=1}^{(p-1)/2} j = \left(\frac{p-1}{2}\right)!$$

é uma solução de $x^2 \equiv -1(\text{mod } p)$.

Suponhamos, agora, que a congruência $x^2 \equiv -1(\text{mod } p)$ tenha solução e que $p > 2$. Elevando ambos os membros à potência $(p-1)/2$ obtemos:

$$(x^2)^{(p-1)/2} \equiv (-1)^{(p-1)/2}(\text{mod } p).$$

Como $(x^2)^{(p-1)/2} \equiv x^{(p-1)}(\text{mod } p)$, pelo Teorema 2.11 (observe que $p \nmid x$ pois $x^2 \equiv -1(\text{mod } p)$) temos que

$$(-1)^{(p-1)/2} \equiv 1(\text{mod } p).$$

Logo $(p-1)/2$ é par, ou seja, $p \equiv 1(\text{mod } 4)$. □

Este resultado que acabamos de provar será demonstrado na próxima seção fazendo-se uso do critério de Euler.

5.2 Símbolo de Legendre e o Critério de Euler

Definição 5.2. Para p um primo ímpar e a um inteiro não-divisível por p, definimos o *Símbolo de Legendre* $\left(\frac{a}{p}\right)$ por

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{se } a \text{ é um resíduo quadrático de } p \\ -1, & \text{se } a \text{ não é um resíduo quadrático de } p \end{cases}$$

Exemplo 5.1 Como as congruências $x^2 \equiv 1(\text{mod } 7), x^2 \equiv 2(\text{mod } 7)$ e $x^2 \equiv 4(\text{mod } 7)$ possuem soluções temos que

$$\left(\frac{1}{7}\right) = \left(\frac{2}{7}\right) = \left(\frac{4}{7}\right) = 1.$$

Por outro lado,

$$\left(\frac{3}{7}\right) = \left(\frac{5}{7}\right) = \left(\frac{6}{7}\right) = -1$$

uma vez que as congruências $x^2 \equiv 3(\text{mod } 7), x^2 \equiv 5(\text{mod } 7)$ e $x^2 \equiv 6(\text{mod } 7)$ não possuem soluções.

Teorema 5.7 (Critério de Euler) *Se* p *for um primo ímpar e* a *um inteiro não-divisível por* p, *então*

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} (\mathrm{mod}\ p).$$

Demonstração: Vamos supor, primeiramente, que $\left(\frac{a}{p}\right) = 1$. Isto significa que a congruência $x^2 \equiv a (\mathrm{mod}\ p)$ tem solução. Seja y uma solução. Do fato de que $(a, p) = 1$ e $p|(y^2 - a)$ concluímos que $(y, p) = 1$. Logo, pelo Pequeno Teorema de Fermat (Teorema 2.11), $y^{p-1} \equiv 1 (\mathrm{mod}\ p)$ e, portanto,

$$a^{\frac{(p-1)}{2}} \equiv (y^2)^{\frac{(p-1)}{2}} = y^{p-1} \equiv 1 (\mathrm{mod}\ p).$$

Isto prova o teorema no caso em que $\left(\frac{a}{p}\right) = 1$.

Consideremos, agora, o caso $\left(\frac{a}{p}\right) = -1$. Já vimos, na primeira parte, que se a for um resíduo quadrático, $a^{(p-1)/2} \equiv 1 (\mathrm{mod}\ p)$. Pelo Teorema 5.2, a congruência $f(x) = x^{(p-1)/2} - 1 \equiv 0 (\mathrm{mod}\ p)$ possui no máximo $(p-1)/2$ soluções incongruentes módulo p. Mas do fato de existirem $(p-1)/2$ resíduos quadráticos, e de termos $a^{(p-1)/2} \equiv 1 (\mathrm{mod}\ p)$ para todo resíduo quadrático, concluímos que todos eles são soluções de $f(x) \equiv 0 (\mathrm{mod}\ p)$. Isto nos garante que a congruência $f(x) \equiv 0 (\mathrm{mod}\ p)$ possui exatamente $(p-1)/2$ raízes e que, portanto, se a não for resíduo quadrático, i.e., $\left(\frac{a}{p}\right) = -1$, então $a^{(p-1)/2} \not\equiv 1 (\mathrm{mod}\ p)$. Mas, como

$$a^{p-1} - 1 = (a^{(p-1)/2} - 1)(a^{(p-1)/2} + 1)$$

e

$$a^{p-1} - 1 \equiv 0 (\mathrm{mod}\ p), \qquad \text{para} \quad (p, a) = 1,$$

concluímos que $a^{(p-1)/2} \equiv \pm 1 (\mathrm{mod}\ p)$.

Logo, caso $\left(\frac{a}{p}\right) = -1$ deveremos ter $a^{(p-1)/2} \equiv -1 (\mathrm{mod}\ p)$, ou seja,

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} (\mathrm{mod}\ p),$$

o que conclui a demonstração. □

Teorema 5.8 *O Símbolo de Legendre é uma função completamente multiplicativa de* a, *isto é,*

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

para a e b inteiros não-divisíveis por p.

Demonstração: Como vimos no capítulo anterior uma função aritmética $f(n)$ para a qual $f(nm) = f(n)f(m)$ para quaisquer n e m é chamada de completamente multiplicativa . Estamos, aqui, considerando $f(n) = \left(\frac{n}{p}\right)$ onde $(n, p) = 1$. Pelo Critério de Euler,

$$\left(\frac{ab}{p}\right) \equiv (ab)^{(p-1)/2} = a^{(p-1)/2} b^{(p-1)/2} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) (\mathrm{mod}\ p).$$

Como o Símbolo de Legendre pode assumir somente os valores 1 e -1 e p é ímpar, a congruência acima implica a igualdade

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

□

Corolário 5.2 $\left(\frac{a^2}{p}\right) = 1.$

Demonstração: Basta tomar $a = b$ no teorema e considerar o fato de que $\left(\frac{a}{p}\right) = \pm 1$. □

O Teorema 5.7 nos diz que o produto de dois resíduos quadráticos é um resíduo quadrático, que o produto de dois números que não são resíduos quadráticos é um resíduo quadrático e que o produto de um que não é resíduo quadrático por um que é resíduo quadrático não é resíduo quadrático.

Os teoremas seguintes nos permitem caracterizar todos os primos para os quais -1 e 2 são resíduos quadráticos.

Teorema 5.9 *Para* p *um primo ímpar, temos*

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{se } p \equiv 1 (\mathrm{mod}\ 4) \\ -1 & \text{se } p \equiv -1 (\mathrm{mod}\ 4) \end{cases}$$

Demonstração: Pelo Critério de Euler sabemos que

$$\left(\frac{-1}{p}\right) \equiv (-1)^{(p-1)/2} (\mathrm{mod}\ p).$$

Isto nos diz que $\left(\frac{-1}{p}\right)$ será igual a 1 quando $(p-1)/2$ for par e igual a -1, quando $(p-1)/2$ for ímpar. Sendo p um primo ímpar, existem apenas duas possibilidades para p em termos de congruência módulo 4, ou $p \equiv 1 (\text{mod } 4)$ ou $p \equiv 3 (\text{mod } 4)$.

Se $p \equiv 1 (\text{mod } 4)$, então $p-1$, sendo divisível por 4, teremos $(p-1)/2$ par. Se $p \equiv 3 (\text{mod } 4)$, existe k tal que $p-3 = p-1-2 = 4k$ e, portanto, $p-1 = 4k+2 = 2(2k+1)$ o que implica $(p-1)/2$ ímpar.

Logo, para $p \equiv 1 (\text{mod } 4)$, $\left(\frac{-1}{p}\right) = 1$ e, para $p \equiv 3 (\text{mod } 4)$, $\left(\frac{-1}{p}\right) = -1$. □

Como os primos 5, 17, 29 e 37 são todos congruentes a 1 módulo 4, temos

$$\left(\frac{-1}{5}\right) = \left(\frac{-1}{17}\right) = \left(\frac{-1}{29}\right) = \left(\frac{-1}{37}\right) = 1.$$

Para os primos 3, 7, 19 e 31, que são congruentes a 3 módulo 4, temos

$$\left(\frac{-1}{3}\right) = \left(\frac{-1}{7}\right) = \left(\frac{-1}{19}\right) = \left(\frac{-1}{31}\right) = -1.$$

Teorema 5.10 *Para* p *um primo ímpar, temos*

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{se } p \equiv \pm 1 (\text{mod } 8) \\ -1 & \text{se } p \equiv \pm 3 (\text{mod } 8) \end{cases}$$

Demonstração: Pelo Critério de Euler, temos

$$\left(\frac{2}{p}\right) \equiv 2^{(p-1)/2} (\text{mod } p).$$

Provamos, a seguir, que

$$2^{(p-1)/2} \equiv (-1)^{(p^2-1)/8} (\text{mod } p). \tag{5.1}$$

Isto irá garantir nosso resultado pois, sendo p um primo ímpar, p necessariamente deverá ser congruente a 1, 3, 5 ou 7 módulo 8. Verificamos o que ocorre em cada um destes 4 casos antes de demonstrarmos (5.1).

$p \equiv 1 (\text{mod } 8) \Rightarrow p-1 = 8k \Rightarrow p+1 = 8k+2$. Logo,

$$\frac{p^2-1}{8} = \frac{(p+1)(p-1)}{8} = \frac{(8k+2)(8k)}{8} = 2k(4k+1).$$

$p \equiv 7 (\text{mod } 8) \Rightarrow p-7 = 8k \Rightarrow p-1 = 8k+6 \Rightarrow p+1 = 8k+8$. Logo,

$$\begin{aligned} \frac{p^2-1}{8} &= \frac{(p+1)(p-1)}{8} \\ &= \frac{(8k+8)(8k+6)}{8} \\ &= \frac{8(k+1)2(4k+3)}{8} = 2(k+1)(4k+3). \end{aligned}$$

Logo, se $p \equiv \pm 1 (\text{mod } 8)$, $(p^2-1)/8$ é par (lembre-se que $-1 \equiv 7 (\text{mod } 8)$). Verificamos, agora, os casos em que $p \equiv 3$ ou 5 módulo 8. $p \equiv 3 (\text{mod } 8) \Rightarrow p-3 = 8k \Rightarrow p-1 = 8k+2 \Rightarrow p+1 = 8k+4$. Logo,

$$\begin{aligned} \frac{p^2-1}{8} &= \frac{(p+1)(p-1)}{8} = \frac{(8k+4)(8k+2)}{8} \\ &= \frac{4(2k+1)2(4k+1)}{8} = (2k+1)(4k+1). \end{aligned}$$

$p \equiv 5 (\text{mod } 8) \Rightarrow p-5 = 8k \Rightarrow p-1 = 8k+4 \Rightarrow p+1 = 8k+6$. Logo,

$$\begin{aligned} \frac{p^2-1}{8} &= \frac{(p+1)(p-1)}{8} = \frac{(8k+6)(8k+4)}{8} \\ &= \frac{2(4k+3)4(2k+1)}{8} = (4k+3)(2k+1). \end{aligned}$$

Portanto se $p \equiv \pm 3 (\text{mod } 8)$, $(p^2-1)/8$ é ímpar (lembre-se que $-3 \equiv 5 (\text{mod } 8)$).

Para provarmos (5.1), consideramos o fato de que para i ímpar, $p - i \equiv i(-1)^i (\text{mod } p)$ e para i par, $i \equiv i(-1)^i (\text{mod } p)$. Logo, se considerarmos as $(p-1)/2$ congruências

$$\begin{aligned} p-1 &\equiv 1(-1)^1 (\text{mod } p) \\ 2 &\equiv 2(-1)^2 (\text{mod } p) \\ p-3 &\equiv 3(-1)^3 (\text{mod } p) \\ 4 &\equiv 4(-1)^4 (\text{mod } p) \\ p-5 &\equiv 5(-1)^5 (\text{mod } p) \\ &\vdots \\ t &\equiv \frac{(p-1)}{2}(-1)^{(p-1)/2} (\text{mod } p). \end{aligned}$$

Caso $(p-1)/2$ seja par a última congruência acima será

$$t = \frac{(p-1)}{2} \equiv \frac{(p-1)}{2}(-1)^{(p-1)/2} (\text{mod } p)$$

e, caso $(p-1)/2$ seja ímpar, a última congruência será

$$t = p - \frac{(p-1)}{2} \equiv \frac{(p-1)}{2}(-1)^{(p-1)/2}(\text{mod } p).$$

É fácil observar que os números na coluna da esquerda das congruências acima são todos pares. Na realidade temos nesta coluna os pares $2, 4, 6, \ldots, p-1$. Se multiplicarmos, membro a membro, todas estas congruências teremos,

$$2 \cdot 4 \cdot 6 \cdots (p-1) \equiv (-1)^{(1+2+\cdots+(p-1)/2)}\left(\frac{p-1}{2}\right)!(\text{mod } p).$$

Mas, como

$$2 \cdot 4 \cdot 6 \cdots (p-1) = 2^{(p-1)/2}\left(\frac{p-1}{2}\right)!$$

temos

$$2^{(p-1)/2}\left(\frac{p-1}{2}\right)! \equiv (-1)^{(p^2-1)/8}\left(\frac{p-1}{2}\right)!(\text{mod } p).$$

Cancelando-se o termo $((p-1)/2)!$ (lembre-se que $(((p-1)/2)!, p) = 1$), em ambos os lados, obtemos

$$2^{(p-1)/2} \equiv (-1)^{(p^2-1)/8}(\text{mod } p).$$

Logo,

$$\left(\frac{2}{p}\right) \equiv (-1)^{(p^2-1)/8}(\text{mod } p)$$

o que implica

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$$

considerando-se o fato de que ambos os membros da última congruência assumem somente os valores 1 ou -1 e p é ímpar. □

5.3 Lema de Gauss

Antes de demonstrarmos o Lema de Gauss consideramos um caso particular com a finalidade de ilustrar o que será feito na demonstração. Sejam $a = 4$ e $p = 13$. Calculamos os menores resíduos positivos módulo 13 dos seguintes múltiplos de 4 (observe que $6 = (13-1)/2$):
$1 \cdot 4, 2 \cdot 4, 3 \cdot 4, 4 \cdot 4, 5 \cdot 4$ e $6 \cdot 4$.

$$\begin{aligned} 1 \cdot 4 &\equiv 4(\text{mod } 13) \\ 2 \cdot 4 &\equiv 8(\text{mod } 13) \\ 3 \cdot 4 &\equiv 12(\text{mod } 13) \\ 4 \cdot 4 &\equiv 3(\text{mod } 13) \\ 5 \cdot 4 &\equiv 7(\text{mod } 13) \\ 6 \cdot 4 &\equiv 11(\text{mod } 13) \end{aligned}$$

Dentre estes resíduos, que são 3,4,7,8,11 e 12 só dois, 3 e 4, são menores do que $13/2$. Se tomarmos os que são maiores, i.e., 7,8,11 e 12 e considerarmos os números $13-7, 13-8, 13-11$ e $13-12$, teremos 6,5,2 e 1, respectivamente, que juntamente com 3 e 4 são todos os números de 1 a 6.

Na demonstração do Lema de Gauss faremos o que foi feito acima com um primo ímpar qualquer para provarmos que $(-1)^r = \left(\frac{a}{p}\right)$, onde r é o número de resíduos positivos de $1 \cdot a, 2 \cdot a, 3 \cdot a, \cdots, \frac{p-1}{2} \cdot a$ que são maiores do que $p/2$. Neste nosso caso particular $r = 4$, i.e.,

$$\left(\frac{4}{13}\right) = (-1)^4 = 1,$$

o que está em concordância com o Critério de Euler que diz que

$$\left(\frac{4}{13}\right) \equiv 4^{(13-1)/2} \equiv 4^6 \equiv 4^2 \cdot 4^2 \cdot 4^2 \equiv 3 \cdot 3 \cdot 3 \cdot \equiv 1(\text{mod } 13).$$

Lema 5.1 (Lema de Gauss) *Sejam p um primo ímpar e a um inteiro não-divisível por p. Consideremos os menores resíduos positivos dos inteiros*

$$a, 2a, 3a, \ldots, \left(\frac{p-1}{2}\right)a.$$

Se r for o número destes resíduos que são maiores do que $p/2$, então,

$$\left(\frac{a}{p}\right) = (-1)^r.$$

Demonstração: Consideremos os menores resíduos positivos de $1a, 2a, 3a, \ldots, (p-1)a/2$ módulo p. É claro que estes resíduos são todos menores do que p. Sejam $a_1, a_2, \ldots, a_s$ os resíduos que são menores do que $p/2$ e $b_1, b_2, b_3, \ldots, b_r$ os que são maiores do que $p/2$. É claro que se multiplicarmos, membro a membro, todas as $(p-1)/2$ congruências de onde obtivemos os resíduos a_i e b_i acima teremos:

$$1a \cdot 2a \cdot 3a \cdots \frac{(p-1)}{2}a \equiv a_1 a_2 \cdots a_s b_1 b_2 \cdots b_r(\text{mod } p)$$

ou seja

$$a^{\frac{p-1}{2}}\left(\frac{p-1}{2}\right)! \equiv a_1a_2\cdots a_s\cdot b_1b_2\cdots b_r (\text{mod } p) \qquad (5.2)$$

Como os números $b_1, b_2, b_3, \ldots, b_r$ são maiores do que $p/2$ e menores do que p, os números $p-b_1, p-b_2, p-b_3, \ldots, p-b_r$ são todos menores do que $p/2$. Desejamos mostrar que os números $a_1, a_2, \ldots, a_s, p-b_1, p-b_2, p-b_3, \ldots, p-b_r$ são todos incongruentes módulo p. Isto será suficiente para mostrar que eles são, a menos da ordem, os números $1, 2, 3, \ldots, (p-1)/2$, uma vez que $r+s=(p-1)/2$. Se tivéssemos dois a_i's ou dois b_i's congruentes módulo p, teríamos dois elementos do conjunto $\{1a, 2a, \ldots, (p-1)a/2\}$ congruentes módulo p o que é impossível pois $(a,p)=1$ e os números $1, 2, \ldots, (p-1)/2$ são todos menores de que p. Nenhum a_i pode ser congruente com $p-b_j$ pois neste caso teríamos $a_i \equiv -b_j$ o que, após o cancelamento de a (a_i e b_i são, ambos, congruentes a múltiplos de a), em ambos os membros, nos daria uma congruência do tipo $n \equiv -m (\text{mod } p)$ com n e m elementos do conjunto $\{1, 2, \ldots, (p-1)/2\}$, o que é impossível. Com isto concluímos que os números $a_1, a_2, \ldots, a_s, p-b_1, p-b_2, p-b_3, \ldots, p-b_r$ são, a menos da ordem, os números $1, 2, 3, \ldots, (p-1)/2$.

Portanto,

$$a_1a_2\cdots a_s(p-b_1)(p-b_2)\cdots(p-b_r) \equiv 1\cdot 2\cdot 3\cdots\frac{(p-1)}{2} (\text{mod } p)$$

ou seja,

$$a_1a_2\cdots a_s(-1)^r b_1b_2\cdots b_r \equiv \left(\frac{p-1}{2}\right)! (\text{mod } p)$$

isto é

$$(-1)^r a_1a_2\cdots a_s b_1b_2\cdots b_r. \equiv \left(\frac{p-1}{2}\right)! (\text{mod } p).$$

Utilizando-se a congruência (5.2) temos,

$$(-1)^r a^{\frac{p-1}{2}}\left(\frac{p-1}{2}\right)! \equiv \left(\frac{p-1}{2}\right)! (\text{mod } p)$$

e, como, $(((p-1)/2)!, p) = 1$ obtemos,

$$(-1)^r a^{\frac{p-1}{2}} \equiv 1 (\text{mod } p).$$

Agora se utilizarmos o Critério de Euler, após multiplicação de ambos os membros por $(-1)^r$ teremos,

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \equiv (-1)^r (\text{mod } p)$$

donde $\left(\frac{a}{p}\right) = (-1)^r$. □

5.4 Lei de Reciprocidade Quadrática

Iniciamos esta seção com a demonstração do seguinte resultado.

Teorema 5.11 *Se p é um primo ímpar e a um inteiro ímpar não-divisível por p, então,*

$$\left(\frac{a}{p}\right) = (-1)^M$$

onde

$$M = \left\lfloor\frac{a}{p}\right\rfloor + \left\lfloor\frac{2a}{p}\right\rfloor + \left\lfloor\frac{3a}{p}\right\rfloor + \cdots + \left\lfloor\frac{p-1}{2}\cdot\frac{a}{p}\right\rfloor.$$

Demonstração: Pelo Algoritmo da Divisão podemos obter os menores resíduos positivos de $a, 2a, 3a, \ldots, (p-1)a/2$ através das divisões seguintes:

$$a = p\left\lfloor\frac{a}{p}\right\rfloor + r_1$$
$$2a = p\left\lfloor\frac{2a}{p}\right\rfloor + r_2$$
$$3a = p\left\lfloor\frac{3a}{p}\right\rfloor + r_3$$
$$\vdots$$
$$\frac{p-1}{2}a = p\left\lfloor\frac{p-1}{2}\cdot\frac{a}{p}\right\rfloor + r_{(p-1)/2}$$

onde $r_1, r_2, \ldots, r_{(p-1)/2}$são os a_i e b_i definidos na demonstração do Lema 5.1. Se somarmos, membro a membro, as $(p-1)/2$ igualdades acima obteremos

$$a(1+2+3+\cdots+\frac{p-1}{2}) = p\left(\left\lfloor\frac{a}{p}\right\rfloor + \left\lfloor\frac{2a}{p}\right\rfloor + \cdots + \left\lfloor\frac{p-1}{2}\frac{a}{p}\right\rfloor\right) + $$
$$+ r_1 + r_2 + \cdots + r_{(p-1)/2}$$

ou seja

$$\frac{p^2-1}{8}a = pM + I + S \qquad (5.3)$$

onde I e S são, respectivamente, as somas dos resíduos inferiores e superiores a $p/2$, isto é,

$$I = a_1 + a_2 + a_3 + \cdots + a_s$$

e

$$S = b_1 + b_2 + b_3 + \cdots + b_r.$$

Vimos, também, na demonstração do Lema de Gauss (Lema 5.1) que os números $a_1, a_2, \ldots, a_s, p - b_1, p - b_2, \ldots, p - b_r$ são, a menos da ordem, os números $1, 2, 3, \ldots, (p-1)/2$. Logo,

$$\begin{aligned} 1 + 2 + \cdots + \frac{p-1}{2} &= \frac{p^2-1}{8} \\ &= a_1 + a_2 + \cdots + a_s + rp - (b_1 + b_2 + \cdots + b_r) \end{aligned}$$

i.e.,

$$\frac{p^2-1}{8} = I + rp - S. \tag{5.4}$$

Subtraindo-se, membro a membro, as equações (5.3) e (5.4) obtemos

$$\frac{p^2-1}{8}(a-1) = p(M-r) + 2S.$$

Como, por hipótese, a e p são ímpares o termo $(p^2-1)(a-1)/8$ será par e, portanto, $p(M-r)$ também. Logo, $M - r$ é par. Mas, se esta diferença é par, é porque ambos são pares ou ambos são ímpares. Portanto, pelo Lema de Gauss, concluímos que

$$\left(\frac{a}{p}\right) = (-1)^r = (-1)^M$$

uma vez que M e r possuem a mesma paridade. □

Observação: Dizemos que dois inteiros possuem a mesma paridade quando são ambos pares ou ambos ímpares.

O resultado que apresentamos a seguir, chamado "Lei de Reciprocidade Quadrática" de Gauss, já foi demonstrado de várias formas distintas. O próprio Gauss forneceu pelo menos 8 demonstrações e a literatura menciona mais de 150. Este resultado já era conhecido por Euler e Legendre.

Para p e q primos ímpares, esta Lei de Reciprocidade Quadrática nos diz que as congruências $x^2 \equiv p \pmod q$ e $x^2 \equiv q \pmod p$ são ambas solúveis ou ambas insolúveis, a menos que p e q sejam congruentes a 3 módulo 4, caso

em que uma terá solução e a outra não. Isto pode ser expresso em termos do Símbolo de Legendre, como mostra o enunciado do teorema seguinte.

Teorema 5.12 (Lei de Reciprocidade Quadrática) *Se p e q são primos ímpares distintos, então*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

Demonstração: Esta demonstração, usando argumentos geométricos, foi apresentada, originalmente, por Eisenstein (1823-1852).

Consideremos o retângulo ABCD de vértices $(0,0), (p/2, 0), (p/2, q/2)$ e $(0, q/2)$. Marcamos, em seu interior, os pontos que pertencem ao produto cartesiano dos conjuntos $\{1, 2, 3, \ldots, (p-1)/2\}$ e $\{1, 2, 3, \ldots, (q-1)/2\}$, conforme figura abaixo.

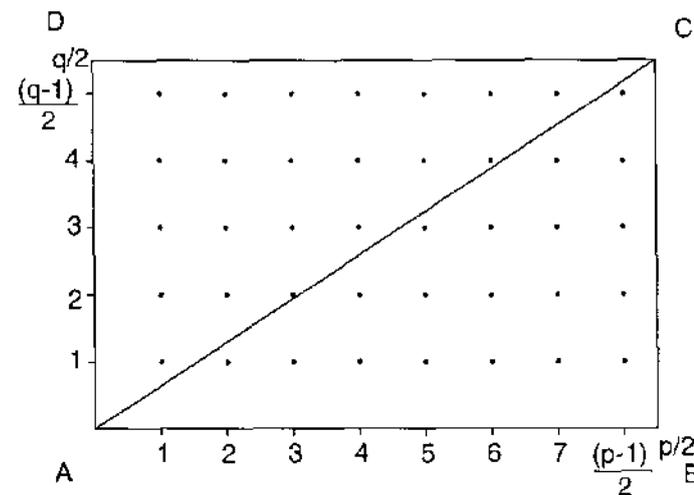



Figura 5.1

É claro que o número de pontos interiores a este retângulo, cujas coordenadas são números inteiros, é igual a

$$\frac{p-1}{2}\frac{q-1}{2}.$$

Consideremos a equação da reta que passa por A e C, i.e., $y = (q/p)x$. Como os números $1, 2, \ldots, (p-1)/2$ são todos primos com p, esta reta não contém

nenhum dos pontos interiores que contamos acima. Esta reta, $y = (q/p)x$, intercepta as retas $x = k$, paralelas ao eixo y, nos pontos $(k, kq/p)$. Como $\frac{kq}{p}$ não é inteiro, para $k \in \{1, 2, 3, \ldots, (p-1)/2\}$, o número $\left\lfloor \frac{kq}{p} \right\rfloor$ é o número de pontos da reta $x = k$ que estão acima do eixo x e abaixo da reta $y = (q/p)x$. Logo, o total M de pontos do nosso reticulado no interior do triângulo ABC é dado por

$$M = \left\lfloor \frac{q}{p} \right\rfloor + \left\lfloor \frac{2q}{p} \right\rfloor + \left\lfloor \frac{3q}{p} \right\rfloor + \cdots + \left\lfloor \frac{p-1}{2} \cdot \frac{q}{p} \right\rfloor.$$

Se considerarmos, agora, as interseções das retas $y = k$, paralelas ao eixo x, com a reta $y = (q/p)x$, obteremos, através de raciocínio análogo ao anterior, que o número N dos pontos, que estamos considerando, no interior do triângulo ACD é igual a

$$N = \left\lfloor \frac{p}{q} \right\rfloor + \left\lfloor \frac{2p}{q} \right\rfloor + \left\lfloor \frac{3p}{q} \right\rfloor + \cdots + \left\lfloor \frac{q-1}{2} \cdot \frac{p}{q} \right\rfloor.$$

Portanto temos a seguinte igualdade,

$$M + N = \frac{p-1}{2}\frac{q-1}{2}.$$

Mas, pelo Teorema 5.11,

$$\left(\frac{q}{p}\right) = (-1)^M \qquad \text{e} \qquad \left(\frac{p}{q}\right) = (-1)^N$$

o que implica

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{M+N} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

□

Finalizamos esta seção com um resultado que será fundamental na demonstração de um teorema de Lagrange visto no capítulo 7.

Teorema 5.13 *Para todo primo p existem inteiros a, b e c, não todos nulos, tais que a congruência seguinte se verifica*

$$a^2 + b^2 + c^2 \equiv 0 (\text{mod } p).$$

Demonstração: Para o caso $p = 2$ tomamos $a = b = 1$ e $c = 0$. Se $p \equiv 1(\text{mod } 4)$ tomamos $b = 1$, $c = 0$ e a como uma solução de $x^2 \equiv -1(\text{mod } p)$ (lembre-se de que o Teorema 5.6 nos garante a existência de um tal "a"). Se $p \equiv 3(\text{mod } 4)$ tomamos $c = 1$ e mostramos a existência de solução para a congruência

$$a^2 + b^2 \equiv -1(\text{mod } p).$$

Sabemos, pelo Teorema 5.5, que para um p primo ímpar temos $(p-1)/2$ resíduos quadráticos e $(p-1)/2$ resíduos não-quadráticos dentre os números $1, 2, 3, \ldots, p-1$.

Seja, pois, d o menor resíduo positivo não-quadrático módulo p. Como 1 é resíduo quadrático, $d \geq 2$. Logo, pelos Teoremas 5.8 e 5.9

$$\left(\frac{-d}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{d}{p}\right) = (-1)(-1) = 1.$$

Isto nos diz que $-d$ é um resíduo quadrático módulo p, ou seja, a congruência $x^2 \equiv -d(\text{mod } p)$ possui solução. Seja b tal que $b^2 \equiv -d(\text{mod } p)$. Precisamos achar um "$a$" tal que $a^2 \equiv d - 1(\text{mod } p)$. Mas esta congruência claramente possui solução uma vez que $d \geq 2$, $d - 1 < d$ e d é o menor resíduo não-quadrático positivo módulo p. □

5.5 Símbolo de Jacobi

O Símbolo de Jacobi que definimos a seguir é uma generalização do Símbolo de Legendre introduzido neste capítulo. Este símbolo de Jacobi possui várias propriedades similares àquelas verificadas pelo Símbolo de Legendre. Como veremos este novo Símbolo é de grande importância, na realidade, na avaliação do Símbolo de Legendre.

Definição 5.3 Para um inteiro positivo a relativamente primo com o inteiro ímpar $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_t^{\alpha_t}$ o *Símbolo de Jacobi*, denotado por $\left[\frac{a}{n}\right]$, é definido por:

$$\left[\frac{a}{n}\right] = \left[\frac{a}{p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_t^{\alpha_t}}\right] = \left(\frac{a}{p_1}\right)^{\alpha_1} \left(\frac{a}{p_2}\right)^{\alpha_2} \cdots \left(\frac{a}{p_t}\right)^{\alpha_t}$$

onde os símbolos à direita da última igualdade são Símbolos de Legendre. Para exemplificar a avaliação deste novo símbolo calculamos, a seguir, $\left[\frac{2}{539}\right]$

e $\left[\frac{144}{385}\right]$.

$$\left[\frac{2}{539}\right] = \left[\frac{2}{7^2.11}\right] = \left(\frac{2}{7}\right)^2 \cdot \left(\frac{2}{11}\right) = (1)^2(-1) = -1.$$

$$\left[\frac{144}{385}\right] = \left[\frac{144}{5.7.11}\right] = \left(\frac{144}{5}\right) \cdot \left(\frac{144}{7}\right) \cdot \left(\frac{144}{11}\right)$$
$$= \left(\frac{4}{5}\right) \cdot \left(\frac{4}{7}\right) \cdot \left(\frac{1}{11}\right) = \left(\frac{2}{5}\right)^2 \cdot \left(\frac{2}{7}\right)^2 \cdot \left(\frac{1}{11}\right) = 1.$$

Pela definição acima podemos ver que quando n é primo o Símbolo de Jacobi coincide com o de Legendre.

É importante observar que, enquanto o Símbolo de Legendre $\left(\frac{a}{p}\right)$ nos dá informação sobre a existência de soluções para a congruência $x^2 \equiv a (\text{mod } p)$, o Símbolo de Jacobi $\left[\frac{a}{n}\right]$ não nos fornece semelhante informação sobre a congruência $x^2 \equiv a (\text{mod } n)$. Para ver isto observe que se p é um fator primo de n e se $x^2 \equiv a (\text{mod } n)$ tem solução, então a congruência $x^2 \equiv a (\text{mod } p)$ também tem solução, i.e., $\left(\frac{a}{p}\right) = 1$. Desta forma

$$\left[\frac{a}{n}\right] = \prod_{i=1}^{t} \left(\frac{a}{p_i}\right)^{\alpha_i} = 1.$$

Para mostrar, por outro lado, a possibilidade de se ter $\left[\frac{a}{n}\right] = 1$ sem que a congruência $x^2 \equiv a (\text{mod } n)$ possua solução, consideramos $a = 2$ e $n = 55$. Logo,

$$\left[\frac{2}{55}\right] = \left(\frac{2}{5}\right) \cdot \left(\frac{2}{11}\right) = (-1)(-1) = 1$$

e, como as congruências $x^2 \equiv 2 (\text{mod } 5)$ e $x^2 \equiv 2 (\text{mod } 11)$ não possuem nenhuma solução, a congruência $x^2 \equiv 2 (\text{mod } 55)$ não tem solução alguma.

Provaremos, a seguir, uma propriedade satisfeita pelo Símbolo de Jacobi que usaremos para mostrar que a Lei de Reciprocidade Quadrática também se verifica para o Símbolo de Jacobi.

Teorema 5.14 *O Símbolo de Jacobi satisfaz*

$$\left[\frac{-1}{n}\right] = (-1)^{(n-1)/2}$$

onde n é um inteiro ímpar e positivo.

Demonstração: Sabemos, pelo Teorema 5.9, que se p é um primo ímpar, então

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}.$$

Considerando $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_t^{\alpha_t}$, temos:

$$\left[\frac{-1}{n}\right] = \left(\frac{-1}{p_1}\right)^{\alpha_1} \left(\frac{-1}{p_2}\right)^{\alpha_2} \cdots \left(\frac{-1}{p_t}\right)^{\alpha_t}$$
$$= (-1)^{\alpha_1(p_1-1)/2 + \alpha_2(p_2-1)/2 + \cdots + \alpha_t(p_t-1)/2} \qquad (5.5)$$

Da fatoração de n podemos escrever

$$n = (1 + (p_1 - 1))^{\alpha_1} (1 + (p_2 - 1))^{\alpha_2} \dots (1 + (p_t - 1))^{\alpha_t}.$$

Como $(p_i - 1)$ é par concluímos que $(1 + (p_i - 1))^{\alpha_i} \equiv 1 + \alpha_i(p_i - 1) (\text{mod } 4)$ e $(1 + \alpha_i(p_i - 1))(1 + \alpha_j(p_j - 1)) \equiv 1 + \alpha_i(p_i - 1) + \alpha_j(p_j - 1) (\text{mod } 4)$. Portanto $n \equiv 1 + \alpha_1(p_1 - 1) + \alpha_2(p_2 - 1) + \cdots + \alpha_t(p_t - 1) (\text{mod } 4)$ o que implica

$$\frac{(n-1)}{2} \equiv \frac{\alpha_1(p_1 - 1)}{2} + \frac{\alpha_2(p_2 - 1)}{2} + \cdots + \frac{\alpha_t(p_t - 1)}{2} (\text{mod } 2). \qquad (5.6)$$

Esta última congruência para $(n-1)/2$ juntamente com (5.5) nos mostra que

$$\left[\frac{-1}{n}\right] = (-1)^{(n-1)/2}$$

o que conclui a demonstração. □

No Teorema seguinte mostramos que a Lei de Reciprocidade Quadrática é verificada pelo Símbolo de Jacobi.

Teorema 5.15 *Sejam n e m inteiros ímpares positivos relativamente primos, então*

$$\left[\frac{n}{m}\right] \left[\frac{m}{n}\right] = (-1)^{\frac{m-1}{2} \cdot \frac{n-1}{2}}.$$

Demonstração: Escrevendo $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_t^{\alpha_t}$ e $m = q_1^{\beta_1} q_2^{\beta_2} \cdots q_s^{\beta_s}$, pela definição do Símbolo de Jacobi e pelo Teorema 5.8 temos

$$\left[\frac{n}{m}\right] = \prod_{j=1}^{s} \left(\frac{n}{q_j}\right)^{\beta_j} = \prod_{i=1}^{t} \prod_{j=1}^{s} \left(\frac{p_i}{q_j}\right)^{\beta_j \alpha_i}$$

e

$$\left[\frac{m}{n}\right] = \prod_{i=1}^{t}\left(\frac{m}{p_i}\right)^{\alpha_i} = \prod_{j=1}^{s}\prod_{i=1}^{t}\left(\frac{q_j}{p_i}\right)^{\alpha_i\beta_j}.$$

Logo

$$\left[\frac{n}{m}\right]\left[\frac{m}{n}\right] = \prod_{i=1}^{t}\prod_{j=1}^{s}\left\{\left(\frac{p_i}{q_i}\right)\left(\frac{q_j}{p_i}\right)\right\}^{\alpha_i\beta_j}. \tag{5.7}$$

Como o Símbolo de Legendre verifica a lei de reciprocidade quadrática temos

$$\left(\frac{p_i}{q_j}\right)\left(\frac{q_j}{p_i}\right) = (-1)^{\frac{p_i-1}{2}\frac{q_j-1}{2}}$$

o que, por (5.7), nos fornece

$$\begin{aligned}\left[\frac{n}{m}\right]\left[\frac{m}{n}\right] &= \prod_{i=1}^{t}\prod_{j=1}^{s}(-1)^{\alpha_i(\frac{p_i-1}{2})\beta_j(\frac{q_j-1}{2})} \\ &= (-1)^{\sum_{i=1}^{t}\sum_{j=1}^{s}\alpha_i(\frac{p_i-1}{2})\beta_j(\frac{q_j-1}{2})}.\end{aligned} \tag{5.8}$$

Observando que

$$\sum_{i=1}^{t}\sum_{j=1}^{s}\alpha_i\left(\frac{p_i-1}{2}\right)\beta_j\left(\frac{q_j-1}{2}\right) = \sum_{i=1}^{t}\alpha_i\left(\frac{p_i-1}{2}\right)\sum_{j=1}^{s}\beta_j\left(\frac{q_j-1}{2}\right)$$

e utilizando (5.6) temos:

$$\sum_{i=1}^{t}\alpha_i\left(\frac{p_i-1}{2}\right) \equiv \frac{n-1}{2}(\text{mod } 2)$$

e

$$\sum_{j=1}^{s}\beta_j\left(\frac{q_j-1}{2}\right) \equiv \frac{m-1}{2}(\text{mod } 2)$$

o que nos diz que

$$\sum_{i=1}^{t}\sum_{j=1}^{s}\alpha_i\left(\frac{p_i-1}{2}\right)\beta_j\left(\frac{q_j-1}{2}\right) \equiv \frac{n-1}{2}\frac{m-1}{2}(\text{mod } 2).$$

Esta última congruência nos garante, juntamente com (5.8), que

$$\left[\frac{n}{m}\right]\left[\frac{m}{n}\right] = (-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}}$$

o que conclui a demonstração. □

Dentre os problemas resolvidos da próxima seção estão algumas outras propriedades verificadas pelo Símbolo de Jacobi que já vimos serem satisfeitas pelo Símbolo de Legendre.

5.6 Problemas Resolvidos

Problema 5.1 Mostrar que se $(ab, n) = 1$, onde n é inteiro ímpar positivo, então

$$\left[\frac{ab}{n}\right] = \left[\frac{a}{n}\right]\left[\frac{b}{n}\right]$$

Solução: Escrevendo $n = p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_t^{\alpha_t}$, temos

$$\begin{aligned}\left[\frac{ab}{n}\right] &= \prod_{i=1}^{t}\left(\frac{ab}{p_i}\right)^{\alpha_i} = \prod_{i=1}^{t}\left(\frac{a}{p_i}\right)^{\alpha_i}\cdot\left(\frac{b}{p_i}\right)^{\alpha_i} \\ &= \prod_{i=1}^{t}\left(\frac{a}{p_i}\right)^{\alpha_i}\prod_{i=1}^{t}\left(\frac{b}{p_i}\right)^{\alpha_i} \\ &= \left[\frac{a}{n}\right]\left[\frac{b}{n}\right]\end{aligned}$$

Problema 5.2 Mostrar que se n for um inteiro ímpar e positivo então

$$\left[\frac{2}{n}\right] = (-1)^{(n^2-1)/8}$$

Solução: Sabemos, pelo Teorema 5.10, que para p primo

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}.$$

Logo,

$$\left[\frac{2}{n}\right] = \left(\frac{2}{p_1}\right)^{\alpha_1}\left(\frac{2}{p_2}\right)^{\alpha_2}\cdots\left(\frac{2}{p_t}\right)^{\alpha_t}$$

$$= (-1)^{\alpha_1(p_1^2-1)/8+\alpha_2(p_2^2-1)/8+\cdots+\alpha_t(p_t^2-1)/8} \qquad (5.9)$$

Como foi observado na demonstração do Teorema 5.14 temos

$$n^2 = (1+(p_1^2-1))^{\alpha_1}(1+(p_2^2-1))^{\alpha_2}\cdots(1+(p_t^2-1))^{\alpha_t}.$$

Considerando que $p_i^2 - 1 \equiv 0 \pmod 8$ vemos que

$$(1+(p_i^2-1))^{\alpha_i} \equiv 1 + \alpha_i(p_i^2-1) \pmod{64}$$

e

$$(1+\alpha_i(p_i^2-1))(1+\alpha_j(p_j^2-1)) \equiv 1 + \alpha_i(p_i^2-1) + \alpha_j(p_j^2-1) \pmod{64}$$

Logo,

$$n^2 \equiv 1 + \alpha_1(p_1^2-1) + \alpha_2(p_2^2-1) + \cdots + \alpha_t(p_t^2-1) \pmod{64}$$

o que nos garante que

$$\frac{n^2-1}{8} \equiv \frac{\alpha_1(p_1^2-1)}{8} + \frac{\alpha_2(p_2^2-1)}{8} + \cdots + \frac{\alpha_t(p_t^2-1)}{8} \pmod 8.$$

Esta última congruência, com (5.9), nos permite concluir, finalmente, que

$$\left[\frac{2}{n}\right] = (-1)^{\frac{n^2-1}{8}}.$$

Problema 5.3 Avaliar o Símbolo de Legendre $\left(\frac{497}{643}\right)$.

Solução: Vamos avaliar este Símbolo de Legendre considerando-o como Símbolo de Jacobi para que possamos utilizar o fato de que este símbolo também satisfaz a lei de reciprocidade quadrática:

$$\begin{aligned}
\left(\frac{497}{643}\right) = \left[\frac{497}{643}\right] &= (-1)^{\frac{497-1}{2}\cdot\frac{653-1}{2}}\left[\frac{643}{497}\right] = \left[\frac{643}{497}\right] \\
&= \left[\frac{146}{497}\right] = \left[\frac{2}{497}\right]\left[\frac{73}{497}\right] \\
&= (-1)^{\frac{73-1}{2}\cdot\frac{497-1}{2}}\left[\frac{497}{73}\right] = \left[\frac{497}{73}\right] \\
&= \left[\frac{59}{73}\right] = (-1)^{\frac{59-1}{2}\cdot\frac{73-1}{2}}\left[\frac{73}{59}\right] = \left[\frac{14}{59}\right] \\
&= \left[\frac{2}{59}\right]\left[\frac{7}{59}\right] = (-1)^{\frac{59^2-1}{8}}\left[\frac{7}{59}\right] = -\left[\frac{7}{59}\right] \\
&= -(-1)^{\frac{7-1}{2}\cdot\frac{59-1}{2}}\left[\frac{59}{7}\right] = \left[\frac{59}{7}\right] \\
&= \left[\frac{3}{7}\right] = (-1)^{\frac{3-1}{2}\cdot\frac{7-1}{2}}\left[\frac{7}{3}\right] = -\left[\frac{7}{3}\right] \\
&= -\left[\frac{1}{3}\right] = -1
\end{aligned}$$

5.7 Problemas Propostos

1. Calcular $\left(\frac{48}{97}\right), \left(\frac{235}{991}\right), \left(\frac{138}{883}\right)$.

2. Encontrar os resíduos quadráticos e não-quadráticos de 19 e 23.

3. Mostrar que não existe n tal que $7|(4n^2-3)$.

4. Mostrar que se p e q são primos ímpares com $p = q + 4a$ então
i) $\left(\frac{p}{q}\right) = \left(\frac{a}{q}\right)$
ii) $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$

5. Usando o Teorema 5.12 mostrar que se p é um primo ímpar, então

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & \text{se} \quad p \equiv \pm 1 \pmod{12} \\ -1 & \text{se} \quad p \equiv \pm 5 \pmod{12} \end{cases}$$

6. Fornecer uma congruência descrevendo todos os primos para os quais 5 é um resíduo quadrático.

7. Mostrar que 17 é um resíduo quadrático módulo 19 utilizando o Lema de Gauss.

8. Dizer se a congruência $3x^2 \equiv 12 \pmod{13}$ possui, ou não, solução.

9. Avaliar $\left[\frac{327}{635}\right], \left[\frac{429}{563}\right], \left[\frac{181}{991}\right]$.

10. Sendo p e q primos ímpares distintos com $p \equiv q \equiv 3 \pmod 4$ mostrar que p é um resíduo quadrático módulo q se, e somente se, q não é resíduo quadrático módulo p.

Capítulo 6

Raízes Primitivas

6.1 Raízes Primitivas

A importância dos resultados introduzidos neste capítulo fica evidente quando se estuda os conceitos de grupos, grupos cíclicos, etc, o que é visto, em maiores detalhes, em Teoria Algébrica de Números que não será desenvolvida neste texto.

Sabemos, pelo Teorema de Euler (Teorema 2.13) que se a e $m (m \geq 1)$ são relativamente primos, então $a^{\phi(m)} \equiv 1 (\text{mod } m)$. Isto nos diz que se considerarmos as potências de a, isto é, $a, a^2, a^3, \ldots, a^i, \ldots$ existirá um menor expoente k tal que $a^k \equiv 1 (\text{mod } m)$. Este menor valor de k poderá ser menor do que $\phi(m)$. Como $(2,7) = 1$, o Teorema de Euler nos garante que $2^{\phi(7)} = 2^6 \equiv 1 (\text{mod } 7)$, mas $2^3 \equiv 1 (\text{mod } 7)$ e $3 < 6 = \phi(7)$.

Definição 6.1 O menor inteiro positivo k para o qual $a^k \equiv 1 (\text{mod } m)$, onde $(a, m) = 1$, é chamado "*ordem de* a *módulo* m" m e denotado por $\text{ord}_m a$.

Como $2 \not\equiv 1 (\text{mod } 7), 2^2 \not\equiv 1 (\text{mod } 7)$ e, como vimos acima, $2^3 \equiv 1 (\text{mod } 7)$, então $\text{ord}_7 2 = 3$.

Em muitos livros de Teoria dos Números o leitor encontrará, também, os termos "a pertence ao expoente k módulo m"ou "k é o expoente de a módulo m".

Nosso primeiro teorema mostra que se $a^h \equiv 1 (\text{mod } m)$ para algum inteiro positivo h, então h, necessariamente, deverá ser múltiplo de $\text{ord}_m a$.

Teorema 6.1 *Se* $k = \text{ord}_m a$ *e* $a^h \equiv 1 (\text{mod } m)$, *então* $k | h$.

Demonstração: Pelo algoritmo da divisão (Teorema 1.2), dados h e $k (k \neq 0)$ existe um único par de inteiros q e r, $0 \leq r < k$ tal que $h = qk + r$. Desta forma, temos

$$a^h = a^{qk+r} = (a^k)^q a^r \equiv a^r (\text{mod } m).$$

Lembre-se que $a^k \equiv 1 (\text{mod } m)$ pois $k = \text{ord}_m a$. Logo, como $a^h \equiv 1 (\text{mod } m)$, acabamos de mostrar que $a^r \equiv 1 (\text{mod } m)$. Sendo $r < k$, r deve ser zero pois k é, por definição, o menor inteiro positivo para o qual $a^k \equiv 1 (\text{mod } m)$. Portanto, $r = 0$ e $h = qk$, o que conclui a demonstração. □

Corolário 6.1: $\text{ord}_m a | \phi(m)$.

Demonstração: O Teorema de Euler (Teorema 2.13) nos garante que $a^{\phi(m)} \equiv 1 (\text{mod } m)$ para $(a, m) = 1$. Logo, o teorema que acabamos de demonstrar nos garante que $\text{ord}_m a | \phi(m)$. □

Definição 6.2 Se $\text{ord}_m a = \phi(m)$ dizemos que a é uma *raiz primitiva* módulo m.

Para calcularmos a $\text{ord}_{10} 3$ computamos, módulo 10, as potências $3, 3^2, 3^3$, etc. $3^1 \equiv 3 (\text{mod } 10); 3^2 \equiv 9 (\text{mod } 10); 3^3 \equiv 7 (\text{mod } 10)$ e $3^4 \equiv 1 (\text{mod } 10)$. Desta forma concluímos que $\text{ord}_{10} 3 = 4$ e, como $4 = \phi(10), 3$ é uma raiz primitiva módulo 10. Pelo Corolário acima, quando estamos procurando a $\text{ord}_m a$, precisamos testar somente as potências cujos expoentes são divisores de $\phi(m)$.

Vamos calcular a $\text{ord}_{10} 7$ e $\text{ord}_{10} 9$. Para isto calculamos as potências de 7 e 9 somente para expoentes que são divisores de $\phi(10) = 4$.

$$\begin{array}{ll} 7^1 \equiv 7 (\text{mod } 10) & 9^1 \equiv 9 (\text{mod } 10) \\ 7^2 \equiv 9 (\text{mod } 10) & 9^2 \equiv 1 (\text{mod } 10) \\ 7^4 \equiv 1 (\text{mod } 10) & \end{array}$$

Como $\text{ord}_{10} 7 = 4 = \phi(10), 7$ é uma raiz primitiva módulo 10. Sendo $\text{ord}_{10} 9 = 2 < 4 = \phi(10), 9$ não é uma raiz primitiva módulo 10.

Chamamos a atenção do leitor para o fato de que se, para algum inteiro positivo $h, a^h \equiv 1 (\text{mod } m)$ então $(a, m) = 1$. Isto é óbvio pois se $d = (a, m)$ então $d | a$ e $d | m$ o que implica $d | 1$ e, portanto, $d = 1$.

Teorema 6.2 *Seja* $k = \text{ord}_m a$, *então* $a^t \equiv a^h (\text{mod } m)$ *se, e somente se,* $t \equiv h (\text{mod } k)$.

Demonstração: Vamos supor que $a^t \equiv a^h (\text{mod } m)$. Sem perda de generalidade podemos supor $t \geq h$. Logo, como $a^t = a^h a^{t-h}$ e $a^h \equiv a^t (\text{mod } m)$ temos $a^h \equiv a^h a^{t-h} (\text{mod } m)$. Como $(a, m) = 1$ implica $(a^h, m) = 1$, podemos cancelar a^h, nesta última congruência, obtendo

$$1 \equiv a^{t-h} (\text{mod } m).$$

Agora, pelo Teorema 6.1, $k | (t - h)$ o que equivale a dizer que $t \equiv h (\text{mod } k)$.

A recíproca é conseqüência do algoritmo da divisão. Se $t \equiv h(\text{mod } k)$ então existe um inteiro n tal que $t = h + nk$. Logo,

$$a^t = a^{h+nk} = a^h(a^k)^n \equiv a^h(\text{mod } m)$$

pois k é a ordem de a módulo m, o que conclui a demonstração. □

Corolário 6.2 *Se $k = \text{ord}_m a$, então os números $1, a, a^2, \dots, a^{k-1}$ são incongruentes módulo m.*

Demonstração: Vamos supor que dois destes números sejam congruentes módulo m, i.e., $a^t \equiv a^h(\text{mod } m)$, $0 \le t \le k-1$, $0 \le h \le k-1$. Pelo Teorema 6.2, devemos ter $t \equiv h(\text{mod } k)$, i.e., $t - h$ deve ser divisível por k. Como ambos, t e h, são não-negativos e menores do que k, isto só poderá ocorrer se eles forem iguais. Disto concluímos que os números $1, a, a^2, \dots, a^{k-1}$ são todos incongruentes módulo m. □

Teorema 6.3 *Se a é uma raiz primitiva, então os números $a, a^2, \dots, a^{\phi(m)}$ formam um sistema reduzido de resíduos módulo m.*

Demonstração: Como a é uma raiz primitiva $\text{ord}_m a = \phi(m)$. Pelo corolário 6.2 $1, a, a^2, \dots, a^{\phi(m)-1}$ são todos incongruentes módulo m. Como $(a, m) = 1$, o Teorema 2.12 nos garante que $a, a^2, \dots, a^{\phi(m)}$ formam um sistema reduzido de resíduos módulo m. □

Teorema 6.4 *Para k inteiro, $k \ge 3$, e a um inteiro ímpar, temos*

$$a^{\phi(2^k)/2} \equiv 1(\text{mod } 2^k). \tag{6.1}$$

Demonstração: A demonstração é por indução. Vamos verificar a validade de (6.1) para $k = 3$. Como a é ímpar, $a = 2n + 1$. Logo,

$$a^2 = (2n+1)^2 = 4n^2 + 4n + 1 = 4n(n+1) + 1.$$

Como $n(n+1)$ é par, $4n(n+1)$ é divisível por 8 e, portanto, $a^2 \equiv 1(\text{mod } 8)$. Isto prova (6.1) para $k = 3$, pois $\phi(2^3)/2 = 2$.

Vamos supor, agora, que

$$a^{\phi(2^k)/2} = a^{2^{k-2}} \equiv 1(\text{mod } 2^k).$$

Isto é equivalente a $a^{2^{k-2}} = 1 + m2^k$ para algum inteiro m. Elevando-se ambos os membros ao quadrado obtemos,

$$(a^{2^{k-2}})^2 = (1 + m2^k)^2 = 1 + m2^{k+1} + m^2 2^{2k}.$$

Portanto,

$$a^{2^{k-1}} = 1 + 2^{k+1}(m + m^2 2^{k-1}),$$

o que implica

$$a^{2^{k-1}} \equiv 1(\text{mod } 2^{k+1})$$

que é (6.1) para k substituído por $k+1$, o que conclui a demonstração. □

A congruência (6.1) nos fala a respeito da não-existência de raízes primitivas módulo 2^k, para $k \ge 3$.

Proposição 6.1 *Para $k = \text{ord}_m a$ e t um inteiro positivo temos,*

$$\text{ord}_m a = (k, t)\text{ord}_m(a^t).$$

Demonstração: Por definição, a ordem de a^t módulo m é o menor inteiro positivo h tal que

$$(a^t)^h = a^{th} \equiv 1(\text{mod } m).$$

Logo, pelo Teorema 6.1, $th \equiv 0(\text{mod } k)$. Esta última congruência, pelo Teorema 2.3, é equivalente a $h \equiv 0(\text{mod } k/d)$ onde $d = (k, t)$.

É claro que a menor solução positiva desta congruência é k/d, o que significa que $\text{ord}_m a^t = k/d$ o que conclui a demonstração. □

Corolário 6.3 $\text{ord}_m a^t = \text{ord}_m a$ *se, e somente se,* $(k, t) = 1$, *onde* $k = \text{ord}_m a$.

Demonstração: É óbvio pela equação

$$\text{ord}_m a = (k, t)\text{ord}_m a^t$$

que a igualdade $\text{ord}_m a = \text{ord}_m a^t$ ocorrerá se, e somente se, $(k, t) = 1$. □

Corolário 6.4 *Seja a uma raiz primitiva módulo m. Nestas condições a^t é uma raiz primitiva módulo m se, e somente se, $(t, \phi(m)) = 1$.*

Demonstração: Se a é uma raiz primitiva, $k = \phi(m)$ e, portanto, pelo corolário anterior $\text{ord}_m a^t = \phi(m)$ se, e somente se, $(t, \phi(m)) = 1$. □

Teorema 6.5 *Um inteiro positivo m que possui uma raiz primitiva, possui exatamente $\phi(\phi(m))$ raízes primitivas incongruentes.*

Demonstração: Sabemos, pelo Teorema 6.3, que sendo a uma raiz primitiva, os números $a, a^2, \dots, a^{\phi(m)}$ formam um sistema reduzido de resíduos módulo m. O corolário anterior nos diz que a^t é uma raiz primitiva se, e somente se,

$(t, \phi(m)) = 1$. Mas o número de t's satisfazendo $(t, \phi(m)) = 1$, $1 \le t \le \phi(m)$ é $\phi(\phi(m))$ e isto conclui a demonstração.

□

Teorema 6.6 *Seja* p *um primo ímpar e* d *um divisor positivo de* $p-1$. *Então o número de inteiros incongruentes módulo* p *tendo ordem igual a* d *é* $\phi(d)$.

Demonstração: No capítulo 4, Teorema 4.5, mostramos que

$$\sum_{d|n} \phi(d) = n.$$

Logo, para os divisores de $p-1$ temos,

$$\sum_{d|p-1} \phi(d) = p-1. \tag{6.2}$$

Separamos o conjunto $1, 2, 3, \ldots, p-1$ em classes A_d, uma para cada divisor de $p-1$. Na classe A_d colocamos todos os elementos a tais que $\mathrm{ord}_p a = d$. É claro que estes conjuntos são disjuntos e que cada um dos elementos $1, 2, 3, \ldots, p-1$ se encontra em algum A_d. Isto significa que, se $g(d)$ for o número de elementos em A_d, então,

$$\sum_{d|p-1} g(d) = p-1. \tag{6.3}$$

Subtraindo (6.3) de (6.2) obtemos,

$$\sum_{d|p-1} (\phi(d) - g(d)) = 0$$

Desejamos mostrar que $g(d) = \phi(d)$ para todo divisor d de $p-1$. Para isto basta mostrarmos que $g(d) \le \phi(d)$. Provar isto equivale a mostrar que se $g(d) \ne 0$, então $g(d)$ deve ser igual a $\phi(d)$. Vamos, pois, supor $g(d) \ne 0$, i.e., A_d não-vazio. Seja $a \in A_d$. Logo $\mathrm{ord}_p a = d$, i.e., $a^d \equiv 1 \pmod p$. O Corolário 6.2 e o Teorema 2.12 nos garantem que os números $a, a^2, \ldots, a^d$ são todos incongruentes módulo p. Mas todas estas potências de a são soluções de $x^d \equiv 1 \pmod p$ e, como pelo Teorema de Lagrange (Teorema 5.2), sendo p primo $x^d - 1 \equiv 0 \pmod p$ tem no máximo d soluções, estes d números $a, a^2, \ldots, a^d$ são todas as soluções de $x^d - 1 \equiv 0 \pmod p$. Logo, todo elemento de A_d é da forma a^t para algum $t \in \{1, 2, \ldots, d\}$. Mas, pelo Corolário 6.3, $\mathrm{ord}_p a^t = \mathrm{ord}_p a = d$ se, e somente se, $(t, d) = 1$. Portanto, dentre os números $a, a^2, \ldots, a^d$ existem exatamente $\phi(d)$ com ordem igual a d. Isto nos garante que $g(d) = \phi(d)$, o que conclui a demonstração. □

6.2 Raízes Primitivas módulo p^t

Teorema 6.7 *Todo número primo ímpar possui uma raiz primitiva.*

Demonstração: Isto é conseqüência imediata do teorema anterior porque $\phi(p) = p-1$ sendo um divisor de $p-1$, existem $\phi(\phi(p)) = \phi(p-1)$ raízes primitivas módulo p. □

Proposição 6.2 *Se* a *é uma raiz primitiva módulo* p, *então* $a+p$ *também é.*

Demonstração: Devemos mostrar que $\mathrm{ord}_p(a+p) = \phi(p)$. Vamos supor que $(a+p)^n \equiv 1 \pmod p$ para $n < \phi(p)$. Como $(a+p)^n \equiv a^n \pmod p$, isto seria absurdo pois, por hipótese, a é raiz primitiva. Logo, a ordem de $a+p$ deve ser, $\phi(p)$ ou seja, $a+p$ também é raiz primitiva módulo p. □

Proposição 6.3 *Existe* a, *raiz primitiva módulo* p, p *primo ímpar, para a qual a seguinte relação se verifica:*

$$a^{p-1} \not\equiv 1 \pmod{p^2} \tag{6.4}$$

Demonstração: O teorema anterior nos garante a existência de uma raiz primitiva para todo primo ímpar. Seja a uma raiz primitiva módulo p. Se a verifica (6.4) não há nada a demonstrar. Se a não verifica (6.4), vamos mostrar que $b = a+p$ a qual, pela proposição anterior, é uma raiz primitiva módulo p satisfaz (6.4).

$$\begin{aligned} b^{p-1} = (a+p)^{p-1} &= \sum_{i=0}^{p-1} \binom{p-1}{i} a^{p-1-i} p^i \\ &= a^{p-1} + (p-1)a^{p-2}p + \sum_{i=2}^{p-1} \binom{p-1}{i} a^{p-1-i} p^i. \end{aligned}$$

É fácil observar que todo termo da última soma acima possui o fator p^2. Logo, módulo p^2, temos

$$b^{p-1} \equiv 1 + a^{p-2}(p^2 - p) \equiv 1 - pa^{p-2} \pmod{p^2}.$$

(lembre-se que, como a não satisfaz (6.4), $a^{p-1} \equiv 1 \pmod{p^2}$). Isto implica que $b^{p-1} \not\equiv 1 \pmod{p^2}$ pois a congruência $pa^{p-2} \equiv 0 \pmod{p^2}$ não pode se verificar uma vez que

$$pa^{p-2} \equiv 0 \pmod{p^2} \;\Rightarrow\; a^{p-2} \equiv 0 \pmod p,$$

o que não pode ocorrer sendo a uma raiz primitiva e $(a,p)=1$. Isto mostra que b satisfaz (6.4), o que conclui a demonstração. □

Teorema 6.8 *Se a for uma raiz primitiva módulo p, p primo ímpar, com $a^{p-1} \not\equiv 1 (\mathrm{mod}\ p^2)$, então*

$$a^{\phi(p^{t-1})} \not\equiv 1 (\mathrm{mod}\ p^t) \tag{6.5}$$

para todo $t \geq 2$.

Demonstração: Demonstramos (6.5) por indução em t. Para $t=2$ temos,

$$a^{\phi(p^{2-1})} = a^{\phi(p)} = a^{p-1} \not\equiv 1 (\mathrm{mod}\ p^2)$$

uma vez que estamos admitindo $a^{p-1} \not\equiv 1 (\mathrm{mod}\ p^2)$.

Como hipótese de indução assumimos que (6.5) seja verdadeira para t e vamos provar que esta congruência continua válida quando substituímos t por $t+1$. Como $(a,p)=1$ (a é uma raiz primitiva) temos que $(a,p^{t-1})=1$ e, portanto, pelo Teorema de Euler (Teorema 2.13)

$$a^{\phi(p^{t-1})} \equiv 1 (\mathrm{mod}\ p^{t-1}).$$

Esta congruência nos garante a existência de um inteiro n tal que

$$a^{\phi(p^{t-1})} = 1 + np^{t-1}. \tag{6.6}$$

Este n não é divisível por p, pois se tivéssemos $n = kp$ a última igualdade nos daria

$$a^{\phi(p^{t-1})} = 1 + kp^t$$

o que iria contradizer nossa hipótese de indução. Sabendo que $p \nmid n$, elevamos ambos os membros de (6.6) à potência p.

$$\begin{aligned}
[a^{\phi(p^{t-1})}]^p = a^{p\phi(p^{t-1})} &= (1+np^{t-1})^p \\
&= \sum_{i=0}^{p} \binom{p}{i} (np^{t-1})^i \\
&= \binom{p}{0} + \binom{p}{1} np^{t-1} + \binom{p}{2} n^2 p^{2(t-1)} + \sum_{i=3}^{p} \binom{p}{i} (np^{t-1})^i \\
&= 1 + np^t + \frac{p(p-1)}{2} n^2 p^{2t-2} + S
\end{aligned}$$

$$= 1 + np^t + \frac{p-1}{2} n^2 p^{2t-1} + S.$$

Mas, sendo $3t-3 = t+2t-3 \geq t+1$ para $t \geq 2$, todo termo da soma

$$S = \sum_{i=3}^{p} \binom{p}{i} (np^{t-1})^i$$

possui uma potência de p que é maior do que ou igual a p^{t+1}.

Como $2t-1 \geq t+1$, para $t \geq 2$, a sequência de igualdades acima nos garante, módulo p^{t+1}, que

$$a^{p\phi(p^{t-1})} = a^{\phi(p^t)} \equiv 1 + np^t (\mathrm{mod}\ p^{t+1}).$$

Esta congruência nos garante que

$$a^{\phi(p^t)} \not\equiv 1 (\mathrm{mod}\ p^{t+1})$$

uma vez que $p \nmid n$. Mas isto é (6.5) com $t+1$ no lugar de t, o que conclui a demonstração. □

Teorema 6.9 *Se p é um primo ímpar, então uma raiz primitiva módulo p é também uma raiz primitiva módulo $p^t, \forall t \geq 1$ se, e somente se, $a^{p-1} \not\equiv 1 (\mathrm{mod}\ p^2)$.*

Demonstração: Seja a uma raiz primitiva módulo p e vamos supor que a também seja uma raiz primitiva módulo p^t, para $t \geq 1$. Neste caso teremos, em particular, que a é raiz primitiva módulo p^2 e isto implica que

$$a^{p-1} \not\equiv 1 (\mathrm{mod}\ p^2)$$

pois, caso contrário, teríamos uma contradição, uma vez que $p-1 < p(p-1) = \phi(p^2)$.

Provamos, agora, a recíproca, i.e., vamos admitir que a seja uma raiz primitiva módulo p para a qual $a^{p-1} \not\equiv 1 (\mathrm{mod}\ p^2)$. Devemos mostrar que a é também uma raiz primitiva módulo p^t para todo $t \geq 2$.

Precisamos mostrar que

$$k = \mathrm{ord}_{p^t} a = \phi(p^t).$$

Como $a^k \equiv 1 (\mathrm{mod}\ p^t)$ temos que $a^k \equiv 1 (\mathrm{mod}\ p)$. Isto nos diz, pelo Teorema 6.1, que $\phi(p) | k$. Logo, $k = n\phi(p)$. Mas sendo $k = \mathrm{ord}_{p^t} a$, $k | \phi(p^t)$ e, portanto, $n\phi(p) | \phi(p^t)$. Como $\phi(p^t) = p^{t-1}(p-1)$ temos que,

$$n(p-1) | p^{t-1}(p-1) \Rightarrow n | p^{t-1}.$$

Logo, $n = p^h$, $h \leq t-1$. Portanto, $k = p^h\phi(p) = p^h(p-1)$.

Precisamos mostrar que $h = t-1$. Vamos supor que $h < t-1$, i.e., $h \leq t-2$. Neste caso, teríamos

$$k = p^h(p-1) | p^{t-2}(p-1) = \phi(p^{t-1}).$$

Isto nos diz que $\phi(p^{t-1})$ é um múltiplo de k e, portanto,

$$a^{\phi(p^{t-1})} \equiv 1 (\text{mod } p^t).$$

Mas isto contradiz o Teorema 6.8. Logo, $h = t-1 \Rightarrow n = p^{t-1} \Rightarrow k = p^{t-1}\phi(p) = p^{t-1}(p-1) = \phi(p^t)$. □

6.3 Raízes Primitivas Módulo $2p^t$

Provamos, na seção anterior, a existência de raízes primitivas módulo p^t para p um primo ímpar. Pelo mesmo argumento apresentado na demonstração da Proposição 6.2, podemos concluir que se a for uma raiz primitiva módulo p^t então $a + p^t$ também será uma raiz primitiva módulo p^t. Como um dos números a e $a + p^t$ é, necessariamente, ímpar, p^t possui sempre uma raiz primitiva ímpar.

No teorema seguinte mostramos que uma raiz primitiva ímpar módulo p^t é, também, raiz primitiva módulo $2p^t$.

Teorema 6.10 *Para p um primo ímpar, $2p^t$ possui raiz primitiva.*

Demonstração: Pelas observações feitas acima p^t possui raiz primitiva ímpar. Seja, pois, a uma raiz primitiva ímpar módulo p^t. Vamos provar que a é raiz primitiva módulo $2p^t$. Lembre-se que para ser raiz primitiva módulo $2p^t$, a deve ser primo com $2p^t$, por isto a não pode ser par. Seja $k = \text{ord}_{2p^t} a$. Precisamos mostrar que $k = \phi(2p^t)$. Sabemos que $k | \phi(2p^t)$. Sendo $\phi(2p^t) = \phi(p^t)$, $k | \phi(p^t)$. Mas como $a^k \equiv 1 (\text{mod } 2p^t)$ temos $a^k \equiv 1 (\text{mod } p^t)$. Logo, sendo a uma raiz primitiva módulo p^t, podemos concluir que $\phi(p^t) | k$. Portanto, $k = \phi(2p^t)$ i.e., a é uma raiz primitiva módulo $2p^t$.

6.4 Somente $1, 2, 4, p^t, 2p^t$ Possuem Raízes Primitivas

É de imediata verificação o fato de que os números 1, 2 e 4 possuem raízes primitivas e que, pelo Teorema 6.4, nenhuma potência de 2, maior do que ou igual à terceira possui raiz primitiva. Nas seções 1, 2 e 3 vimos que os primos ímpares, quaisquer potências destes primos e também o dobro destas potências possuem raízes primitivas.

Mostramos, a seguir, que nenhum número m, além de 1, 2, 4, p^t e $2p^t$ (p primo ímpar), possui raiz primitiva.

Teorema 6.11 *Se $m \geq 1$ não é da forma $1, 2, 4, p^t$ e $2p^t$ (p primo ímpar), então m não possui raiz primitiva.*

Demonstração: Seja

$$m = p_1^{t_1} p_2^{t_2} \dots p_s^{t_s}.$$

Vamos supor que m possua uma raiz primitiva. Seja a uma raiz primitiva módulo m. Logo, $(a, m) = 1$ e $\text{ord}_m a = \phi(m)$. Como $(a, m) = 1$, então, $(a, p_i^{t_i}) = 1 \;\; \forall i = 1, 2, \dots, s$ e $t_i \geq 1$. Assim, pelo Teorema de Euler, temos

$$a^{\phi(p_i^{t_i})} \equiv 1 (\text{mod } p_i^{t_i}).$$

Sabemos que

$$\phi(m) = \phi(p_1^{t_1})\phi(p_2^{t_2}) \dots \phi(p_s^{t_s}).$$

Vamos considerar

$$B = [\phi(p_1^{t_1}), \phi(p_2^{t_2}), \dots, \phi(p_s^{t_s})].$$

É claro que

$$a^B \equiv 1 (\text{mod } p_i^{t_i}), \quad \forall i = 1, 2, \dots, s$$

e, portanto, $\phi(m) \leq B$. Logo,

$$\phi(p_1^{t_1})\phi(p_2^{t_2}) \dots \phi(p_s^{t_s}) \leq [\phi(p_1^{t_1}), \phi(p_2^{t_2}), \dots, \phi(p_s^{t_s})]$$

Mas, para que um produto de números seja menor do que ou igual ao mínimo múltiplo comum destes números, estes números, necessariamente, deverão ser relativamente primos dois-a-dois.

Como $\phi(p^t) = p^{t-1}(p-1)$ sabemos que este número é par para p ímpar ou se $p = 2$, $t \geq 2$. Disto concluímos que os números

$$\phi(p_1^{t_1}), \phi(p_2^{t_2}), \dots, \phi(p_s^{t_s})$$

serão primos, dois a dois, somente se $s = 1$ ou $s = 2$ e $m = 2p^t$. O que acabamos de mostrar é que m, caso tenha raiz primitiva, deverá ser de forma p^t ou $2p^t$ (p primo ímpar). Como já provamos que números desta forma possuem raízes primitivas então, ser da forma $1, 2, 4, p^t, 2p^t$ é uma condição necessária e suficiente para que possua raiz primitiva.

6.5 Problemas Resolvidos

Problemas 5.1 Quantas raízes primitivas possui o primo 13? Encontrar um conjunto com este número de raízes primitivas incongruentes módulo 13.

Solução. Sabemos, pelo Teorema 6.5, que o primo 13 possui $\phi(13-1) = \phi(12) = 4$ raízes primitivas módulo 13. Como 2 é uma raíz primitiva módulo 13, temos, pelo Corolário 6.4 que 2^t é raiz primitiva se, e somente se, $(t, \phi(13)) = 1$. Como os inteiros primos com $\phi(13)$ e menores do que 12 são 5, 7 e 11 o conjunto $\{2, 2^5, 2^7, 2^{11}\}$ possui 4 raízes primitivas incongruentes módulo 13.

Problema 5.2. Mostrar que se $\overline{a}$ é um inverso de a módulo m, então $\text{ord}_m a = \text{ord}_m \overline{a}$.

Solução. Seja $r = \text{ord}_m a$ e suponhamos que $s = \text{ord}_m \overline{a} < r$. Logo, como $a\overline{a} \equiv 1 (\text{mod } m)$, temos que $1 \equiv (a\overline{a})^s \equiv (a^s)(\overline{a}^s) \equiv a^s (\text{mod } m)$ o que é uma contradição pois $s < r$ e $r = \text{ord}_m a$.

Problema 5.3. Provar que se a e b são raízes primitivas módulo um primo ímpar p, então ab não é raiz primitiva módulo p.

Solução. Sendo a raiz primitiva módulo p temos que $\phi(p) = p - 1$ é o menor inteiro positivo para o qual $a^{p-1} - 1 \equiv 0 (\text{mod } p)$.

Como

$$a^{p-1} - 1 = \left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right) \equiv 0 (\text{mod } p)$$

concluímos que $a^{\frac{p-1}{2}} \equiv -1 (\text{mod } p)$.

De forma análoga temos que $b^{\frac{p-1}{2}} \equiv -1 (\text{mod } p)$ donde concluímos que $(ab)^{\frac{p-1}{2}} \equiv 1 (\text{mod } p)$, i.e., ab não é raiz primitiva módulo p.

6.6 Problemas Propostos

1. Encontrar uma raiz primitiva módulo (a) 5; (b) 6; (c) 10; (d) 11; (e) 18; (f) 19.

2. Encontrar o número de raízes primitivas dos seguintes primos (a) 5, (d) 17, (a) 11, (d) 23, (a) 13, (d) 31.

3. Mostrar que se m é um inteiro positivo e a um inteiro, $(a, m) = 1$, tal que $\text{ord}_m a = m - 1$, então m é primo.

4. Mostrar que os divisores primos ímpares de um inteiro $n^2 + 1$ são da forma $4k + 1$.

5. Sendo $p > 2$, primo, e $a > 1$ um inteiro, mostrar que os divisores primos ímpares de $a^p + 1$ são divisores de $a + 1$ ou são da forma $2np + 1$.

6. Mostrar que se a é uma raiz primitiva módulo p (primo) com $p \equiv 1 (\text{mod } 4)$, então $-a$ também é raiz primitiva.

7. Mostrar que se a é um resíduo quadrático módulo p primo ímpar, então a não é raiz primitiva módulo p.

Capítulo 7

Representação de Inteiros como Soma de Quadrados

7.1 O Problema de Waring

Num trabalho publicado em 1770, Waring afirmou que todo inteiro positivo é a soma de no máximo 4 quadrados, no máximo 9 cubos e no máximo 19 quartas potências.

Embora ele não tenha apresentado nenhuma demonstração para estas afirmações, às quais deve ter sido levado pela observação de muitos exemplos, provavelmente ele suspeitava da existência, para cada inteiro positivo k, de um inteiro positivo $g(k)$, tal que todo inteiro positivo n pudesse ser expresso como a soma de no máximo $g(k)$ k-ésimas positivas potências.

No mesmo ano de 1770, Lagrange demonstrou que todo inteiro é a soma de no máximo quatro quadrados.

Somente em 1859 é que surgiu uma demonstração para o fato de que todo inteiro é a soma de no máximo 9 cubos. Em 1909 Hilbert provou a existência, para todo k de um inteiro positivo $g(k)$, independente de n, com a propriedade de que todo inteiro n pode ser expresso como a soma de no máximo $g(k)$ k-ésimas potências. A demonstração, por ele apresentada, prova apenas a existência de $g(k)$ mas não fornece informações sobre o valor real de $g(k)$.

Hardy e Littlewood desenvolveram métodos analíticos fornecendo limitantes superiores para $g(k)$ para todo k.

Nas seções seguintes, caracterizamos os inteiros que possuem representação como soma de dois quadrados, demonstramos o teorema de Lagrange sobre a representação de inteiros como soma de quatro quadrados e apresentamos um resultado de Euler que nos diz que certos primos possuem representação única como soma de dois quadrados. Para o leitor interessado noutros resultados,

recomendamos o excelente livro de Grosswald [11].

7.2 Soma de Dois Quadrados

Nesta seção caracterizamos todos os inteiros n para os quais a equação

$$x^2 + y^2 = n \tag{7.1}$$

possui solução em inteiros. Neste resultado, demonstrado primeiramente por Fermat, utilizamos a seguinte identidade, a qual é verdadeira para quaisquer números reais a, b, c e d.

$$(a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2 \tag{7.2}$$

Este fato elementar nos diz que o produto de números que podem ser representados pela soma de dois quadrados também pode ser representado como soma de dois quadrados. Uma forma simples de se verificar (7.2) é pela consideração de complexos $\alpha = a + bi$ e $\beta = d + ci$ lembrando que $\alpha\overline{\alpha}\beta\overline{\beta} = \alpha\beta\ \overline{\alpha\beta}$.

Iniciamos com um resultado no qual identificamos os primos que possuem representação como soma de dois quadrados.

Teorema 7.1 *Sendo p um primo a equação $x^2 + y^2 = p$ possui solução inteira se, e somente se, $p = 2$ ou $p \equiv 1 \pmod 4$.*

Demonstração: Observamos, inicialmente, que $2 = 1^2 + 1^2$. Sabemos que para todo primo ímpar p temos $p \equiv 1 \pmod 4$ ou $p \equiv 3 \pmod 4$.

Como, para todo inteiro a, $a^2 \equiv 0$ ou $1 \pmod 4$ vemos que se $x^2 + y^2 = p$ então $p \equiv 1 \pmod 4$.

Nos resta mostrar que todo p satisfazendo $p \equiv 1 \pmod 4$ pode ser expresso como soma de dois quadrados.

Tomamos, pois, um primo $p \equiv 1 \pmod 4$. Pelo Teorema 5.6 existe x tal que $x^2 \equiv -1 \pmod p$. Com este x definimos a função $f(u, v) = u + xv$ e tomamos $m = \lfloor \sqrt{p} \rfloor$. Como $\sqrt{p}$ não é um inteiro temos $m < \sqrt{p} < m + 1$. Consideramos os pares (u, v) de inteiros onde $0 \le u \le m$ e $0 \le v \le m$. Desta forma vemos que u pode assumir $m + 1$ valores e v, também, pode assumir $m + 1$ valores. Portanto o número total de pares é $(m + 1)^2$. Como $m + 1 > \sqrt{p}$ temos que $(m + 1)^2 > p$, isto é, o total de pares é superior a p. Como um sistema completo de resíduos módulo p possui exatamente p elementos, concluímos que se considerarmos $f(u, v)$ módulo p teremos mais números do que classes de resíduos para colocá-los. Logo, pelo Princípio da Casa dos Pombos, visto no Capítulo 3, existem pelo menos dois pares distintos (u_1, v_1) e (u_2, v_2) com coordenadas satisfazendo $0 \le u_i \le m$ e $0 \le v_i \le m (i = 1, 2)$ para os quais

$$f(u_1, v_1) \equiv f(u_2, v_2) \pmod p.$$

Isto equivale a $u_1 + xv_1 \equiv u_2 + xv_2 \pmod p$, isto é, $u_1 - u_2 \equiv -x(v_1 - v_2) \pmod p$.

Elevando-se ao quadrado ambos os membros desta última congruência temos:

$$(u_1 - u_2)^2 \equiv x^2(v_1 - v_2)^2 \equiv -(v_1 - v_2)^2 \pmod p$$

uma vez que $x^2 \equiv -1 \pmod p$.

Definindo $a = u_1 - u_2$ e $b = v_1 - v_2$ obtemos

$$a^2 + b^2 \equiv 0 \pmod p$$

ou seja, $p|(a^2 + b^2)$. Como os pares (u_1, v_1) e (u_2, v_2) são distintos, a e b não são ambos nulos, isto é, $a^2 + b^2 > 0$.

Sendo u_1 e u_2 inteiros no intervalo $[0, m]$ temos que $a = u_1 - u_2$ satisfaz $-m \leq a \leq m$. Também para $b = v_1 - v_2$ temos $-m \leq b \leq m$ pela mesma razão. Como $m < \sqrt{p}$ concluímos que $|a| < \sqrt{p}$ e $|b| < \sqrt{p}$. Isto nos diz que $a^2 + b^2 < 2p$.

Logo, $a^2 + b^2$ é um inteiro divisível por p e satisfazendo $0 < a^2 + b^2 < 2p$. Como o único inteiro múltiplo de p neste intervalo é p, concluímos que $a^2 + b^2 = p$. □

Este resultado nos permite, agora, identificar todos os inteiros que possuem representação como soma de dois quadrados.

Teorema 7.2 *Um inteiro n pode ser representado como soma de dois quadrados se, e somente se, tiver fatoração da forma*

$$n = 2^{\alpha} p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r} q_1^{\beta_1} q_2^{\beta_2} \ldots q_s^{\beta_s}$$

onde $p_i \equiv 1 \pmod 4$ *e* $q_j \equiv 3 \pmod 4$, $i = 1, 2, \ldots, r$, $j = 1, 2, \ldots, s$ *e todos os expoentes* β_j *são pares.*

Demonstração: Sabemos que $2 = 1^2 + 1^2$ e que pelo Teorema 7.1 todos os p_i's podem ser representados pela soma de dois quadrados. Logo, se todos os β_j's forem pares cada um pode ser escrito como $\beta_i = 2.\beta_i'$ o que nos diz que $q_j^{\beta_j} = (q_j^2)^{\beta_j'}$. Mas $q_j^2 = q_j^2 + 0^2$, ou seja, q_j^2 é soma de dois quadrados.

Disto concluímos, usando a equação (7.2), que se todos os β_j's forem pares, n terá representação como soma de dois quadrados.

Suponhamos, agora, que n possa ser representado como soma de dois quadrados e que algum β_j seja ímpar. Sem perda de generalidade podemos considerar β_1 ímpar. Seja $d = (a, b)$ onde a e b são inteiros tais que $a^2 + b^2 = n$.

Como $d|a$ e $d|b$ temos $a = k_1 d$ e $b = k_2 d$. Sabemos, pelo corolário da Proposição 1.4, que $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$, isto é, $(k_1, k_2) = 1$. Como $d^2|n$, temos $n = kd^2$. Portanto,

$$k = \frac{n}{d^2} = \left(\frac{a}{d}\right)^2 + \left(\frac{b}{d}\right)^2 = k_1^2 + k_2^2.$$

Como estamos supondo β_1 ímpar o expoente de q_1 em k será ímpar pois $k = n/d^2$. Logo, $q_1|k$ e como $(k_1, k_2) = 1$ podemos concluir que

$$(q_1, k_1) = (q_1, k_2) = 1.$$

Logo, pelo Teorema 2.8, existe x tal que $k_1 x \equiv k_2 \pmod{q_1}$ e, portanto

$$0 \equiv k = k_1^2 + k_2^2 \equiv k_1^2 + k_1^2 x^2 \equiv k_1^2(1 + x^2) \pmod{q_1}.$$

Como $q_1 \nmid k_1^2$ temos que $x^2 + 1 \equiv 0 \pmod{q_1}$ ou seja, $x^2 \equiv -1 \pmod{q_1}$. Sendo $q_1 \equiv 3 \pmod 4$ sabemos que esta última congruência não é possível pelo Teorema 5.6. Disto concluímos que todos os β_j's devem ser pares caso n possua representação como soma de dois quadrados.

□

7.3 Soma de Quatro Quadrados

Na demonstração do Teorema de Lagrange, que fornecemos abaixo, vamos utilizar uma identidade semelhante a (7.2) cuja verificação é deixada para o leitor.

$$\begin{aligned}(a^2 + b^2 + c^2 + d^2)(r^2 + s^2 + t^2 + v^2) &= (ar + bs + ct + dv)^2 \\ +(as - br - cv + dt)^2 + (at + bv - cr - ds)^2 &+ (av - bt + cs - dr)^2\end{aligned} \tag{7.3}$$

Esta identidade nos diz, claramente, que o produto de números possuindo representação como soma de quatro quadrados possui, também, representação como soma de quatro quadrados. Feita esta observação nos falta apenas mostrar que todo primo pode ser representado desta forma.

Teorema 7.3 (Lagrange) *Todo inteiro positivo possui representação como soma de quatro quadrados.*

Demonstração: Como observamos acima vamos mostrar que todo primo possui uma tal representação.

Seja p um primo ímpar (lembre-se que $2 = 1^2 + 1^2 + 0^2 + 0^2$). Pelo Teorema 5.13, existem inteiros a, b e c tais que

$$a^2 + b^2 + c^2 \equiv 0 \pmod p \tag{7.4}$$

Esta congruência pode ser reescrita como

$$a^2+b^2+c^2+d^2 = Mp \tag{7.5}$$

onde M é um inteiro e $d = 0$.

A equação (7.5) e o Princípio da Boa Ordem nos garantem a existência de um menor inteiro m satisfazendo (7.5), isto é,

$$a^2+b^2+c^2+d^2 = mp. \tag{7.6}$$

Como em (7.4) estamos trabalhando módulo p e a, b e c estão elevados ao quadrado podemos tomar a, b e c no intervalo $\left[0, \frac{p}{2}\right)$ em (7.4) e (7.5). Logo,

$$mp = a^2+b^2+c^2+d^2 < 4\left(\frac{p}{2}\right)^2 = p^2, \quad \text{isto é,} \quad m < p.$$

Para concluir a demonstração será suficiente provarmos que $m = 1$.

Vamos mostrar que a suposição, $m > 1$, nos leva à obtenção de um inteiro $0 \le m' < m$ o qual, também, nos fornece uma representação para $m'p$ como soma da quatro quadrados, o que contradiz a forma como m foi escolhido.

Separamos em dois casos: m ímpar e m par. Seja $m > 1$ e m ímpar. Em

$$a^2+b^2+c^2+d^2 = mp \tag{7.7}$$

podemos escolher a_1, b_1, c_1 e d_1 no intervalo $\left[0, \frac{m}{2}\right)$ satisfazendo às equações $a_1 \equiv a(\text{mod } m)$, $b_1 \equiv b(\text{mod } m)$, $c_1 \equiv c(\text{mod } m)$ e $d_1 \equiv d(\text{mod } m)$. Desta forma temos $a_1^2+b_1^2+c_1^2+d_1^2 \equiv 0(\text{mod } m)$ o que nos garante a existência de $m' \ge 0$ tal que

$$a_1^2+b_1^2+c_1^2+d_1^2 = m'm. \tag{7.8}$$

Como os inteiros a_1, b_1, c_1 e d_1 são, todos, menores que $\frac{m}{2}$ temos que $m' < m$. A suposição $m' = 0$ nos leva a uma contradição pois se $m' = 0$ então $a_1 = b_1 = c_1 = d_1 = 0$ e, portanto, $a \equiv b \equiv c \equiv d \equiv 0(\text{mod } m)$ o que implica $m^2 | mp$. Como $m^2 | mp$ implica $m|p$ temos uma contradição, pois $1 < m < p$. Logo, $m' \ne 0$. De (7.7), (7.8) e (7.3) temos

$$\begin{aligned} mpm'm = m^2pm' &= (a^2+b^2+c^2+d^2)(a_1^2+b_1^2+c_1^2+d_1^2) \\ &= (aa_1+bb_1+cc_1+dd_1)^2 + (ab_1-ba_1-cd_1+dc_1)^2 \\ &\quad + (ac_1+bd_1-ca_1-db_1)^2 + (ad_1-bc_1+cb_1-da_1)^2. \end{aligned} \tag{7.9}$$

Como $a \equiv a_1, b \equiv b_1, c \equiv c_1$ e $d \equiv d_1(\text{mod } m)$ e $a^2 \equiv aa_1, b^2 \equiv bb_1, c^2 \equiv cc_1$ e $d^2 \equiv dd_1(\text{mod } m)$ vemos que as quatro expressões que estão elevadas ao quadrado do lado direito da última igualdade acima são múltiplas de m. Portanto existem inteiros $\overline{a}, \overline{b}, \overline{c}$ e $\overline{d}$ tais que (7.9) pode ser reescrita como

$$m^2pm' = (\overline{a}m)^2 + (\overline{b}m)^2 + (\overline{c}m)^2 + (\overline{d}m)^2$$

ou seja, $pm' = \overline{a}^2 + \overline{b}^2 + \overline{c}^2 + \overline{d}^2$ onde $m' < m$.

Nos resta mostrar que no caso m par também podemos encontrar $\overline{m} < m$ tal que $\overline{m}p$ é soma de quatro quadrados.

É fácil ver que, para m par, necessariamente os inteiros a, b, c e d devem ser todos pares, dois pares e dois ímpares ou todos ímpares. Em qualquer um destes três casos podemos escolher a, b, c e d satisfazendo $a \equiv b(\text{mod } 2)$ e $c \equiv d(\text{mod } 2)$, o que nos permite escrever

$$p\frac{m}{2} = \left(\frac{a-b}{2}\right)^2 + \left(\frac{a+b}{2}\right)^2 + \left(\frac{c-d}{2}\right)^2 + \left(\frac{c+d}{2}\right)^2.$$

Portanto, tomando $\overline{m} = \frac{m}{2} < m$, obtemos uma expressão para $\overline{m}p$ como soma de quatro quadrados. Pelas observações feitas anteriormente, concluímos que $m = 1$, ou seja, o primo p pode ser expresso como soma de quatro inteiros sendo cada um deles um quadrado. □

7.4 Um Teorema de Unicidade de Euler

Com a finalidade de provarmos que certos primos possuem representação única como soma de dois quadrados, vamos necessitar das seguintes proposições.

Proposição 7.1 *Se um primo $p = c^2 + d^2$ e se existir $q > 1$ tal que $pq = a^2 + b^2$, $(a, b) = 1$, então q é a soma dos quadrados de dois inteiros relativamente primos.*

Demonstração: É claro que se $p = c^2 + d^2$, p primo, então $(c, d) = 1$. Sendo $pq = a^2 + b^2$ temos

$$c^2(a^2+b^2) - a^2(c^2+d^2) = c^2pq - a^2p = kp,$$

onde $k = c^2q - a^2$. Logo,

$$\begin{aligned} kp &= c^2(a^2+b^2) - a^2(c^2+d^2) \\ &= b^2c^2 - a^2d^2 = (bc-ad)(bc+ad) \end{aligned}$$

o que nos diz que p divide pelo menos um dos fatores $(bc - ad)$ e $(bc + ad)$. Temos $bc - ad \neq 0$ pois $bc = ad$ implica que $a = c$ e $b = d$ (lembre-se que $(a, b) = (c, d) = 1$), o que implicaria p e pq iguais.

Se $p|(bc - ad)$ temos $bc - ad = tp$. Sejam

$$\begin{aligned} r &= b - tc \\ s &= a + td \end{aligned} \tag{7.10}$$

Multiplicando-se a primeira das igualdades em (7.10) por "c" e a segunda por "d" temos

$$\begin{aligned} cr &= bc - tc^2 \\ ds &= ad + td^2 \end{aligned}$$

Subtraindo, membro a membro, obtemos

$$cr - ds = (bc - ad) - t(c^2 + d^2) = tp - tp = 0$$

isto é, $cr = ds$, ou seja, $r = d\frac{s}{c}$ e, como $(c, d) = 1, n = \frac{s}{c}$ é inteiro.

Sendo $s = c\frac{s}{c}$ temos que

$$r = nd \qquad \text{e} \qquad s = nc \tag{7.11}$$

Neste caso de (7.10) temos

$$\begin{aligned} pq = a^2 + b^2 &= (nc - td)^2 + (tc + nd)^2 \\ &= (t^2 + n^2)(c^2 + d^2) = p(t^2 + n^2), \end{aligned}$$

e, portanto, $q = (t^2 + n^2)$. O fato de $(t, n) = 1$ segue de (7.10) juntamente com (7.11) uma vez que $(a, b) = 1$.

O caso $p|(bc + ad)$ é semelhante, isto é, se $bc + ad = kp$ definimos

$$\begin{aligned} r &= b - kc \\ s &= a - kd \end{aligned} \tag{7.12}$$

Logo,

$$\begin{aligned} cr &= cb - kc^2 \\ ds &= ad - kd^2 \end{aligned}$$

e, portanto, $cr + ds = bc + ad - k(c^2 + d^2) = kp - kp = 0$. Disto, concluímos que $cr = -ds$, $r = dn$ e $s = -cn$, onde $n = -s/c$.

Levando-se estes valores em (7.12) obtemos

$$\begin{aligned} pq = a^2 + b^2 &= (-cn + kd)^2 + (dn + kc)^2 \\ &= (k^2 + n^2)(c^2 + d^2) = p(k^2 + n^2) \end{aligned}$$

e, portanto, $q = k^2 + n^2$.

A justificativa de que $(k, n) = 1$ segue pela substituição de $r = dn$ e $s = -cn$ em (7.12) mais o fato de $(a, b) = 1$. □

A proposição seguinte é conseqüência imediata da anterior.

Proposição 7.2 *Se pq é a soma dos quadrados de dois inteiros relativamente primos e q não é a soma de dois quadrados de inteiros relativamente primos, então p possui um fator primo que não é a soma de dois quadrados.*

Demonstração: Seja $p = p_1 p_2 \cdots p_n$ onde cada primo $p_i (i = 1, 2, \ldots, n)$ é a soma de dois quadrados. Como $p_1(p_2 p_3 \cdots p_n q) = pq$ é a soma de dois quadrados de inteiros primos entre si, a proposição anterior nos diz que $p_2 p_3 \ldots p_n q$ é a soma de dois quadrados de inteiros relativamente primos. Repetindo este procedimento concluímos que q é a soma de quadrados de inteiros relativamente primos, o que é uma contradição. Disto concluímos que se q não pode ser expresso como soma de quadrados de dois inteiros relativamente primos e pq pode, então p, necessariamente, deve possuir um fator primo que não é soma de quadrados de dois inteiros primos entre si. □

Proposição 7.3 *Se um primo p divide $a^2 + b^2$ com $(a, b) = 1$, então p é a soma de dois quadrados.*

Demonstração: A prova que apresentamos é por contradição utilizando a Proposição 7.2. Suponhamos que p não seja a soma de dois quadrados e que $p|(a^2 + b^2)$ com $(a, b) = 1$.

Como $p \nmid a$ e $p \nmid b$ temos, pelo problema 29 do capítulo 1, que existem q_1, q_2, r_1 e r_2 satisfazendo

$$\begin{aligned} a &= q_1 p \pm r_1, \quad 0 < r_1 \leq \frac{p}{2} \\ b &= q_2 p \pm r_2, \quad 0 < r_2 \leq \frac{p}{2}. \end{aligned}$$

Logo, $r_1^2 + r_2^2 = a^2 + b^2 + mp = Mp \leq \frac{p^2}{2}$.

Como r_1 e r_2 são menores do que p, qualquer divisor comum de r_1 e r_2 deve dividir M. Fazendo, se necessário, estas simplificações obtemos

$$a_1^2 + b_1^2 = np, \quad \text{com} \quad (a_1, b_1) = 1.$$

A Proposição 7.2 nos garante que n possui um fator primo p_1 o qual não é a soma de dois quadrados e satisfaz $p_1 \leq \frac{p}{2}$.

Se repetirmos exatamente o processo descrito acima com p_1 no lugar de p iremos obter um primo $p_2, p_2 < p_1$, o qual não é soma de dois quadrados. Mas esta afirmação contradiz o fato de que os fatores primos de todas as somas de dois números relativamente primos e suficientemente pequenos são expressos como soma de dois quadrados. $(3^2+4^2=5^2, 3^2+2^2=13, 3^2+1^2=10,\ 2^2+1^2=5, 1^2+1^2=2)$. □

Com este resultado podemos, agora, apresentar uma das demonstrações dadas por Euler para a unicidade da representação de certos primos como soma de quadrados.

Teorema 7.4 *Todo primo da forma* $4n+1$ *possui representação única como soma de dois quadrados.*

Demonstração: Pelo Teorema 5.6 sabemos que -1 é um resíduo quadrático para todo primo $p \equiv 1 (\text{mod } 4)$, isto é, que existe um inteiro "a" tal que $a^2 \equiv -1 (\text{mod } p)$ para p primo, $p = 4n+1$.

Logo como $p | a^2+1$ concluímos, pela Proposição 7.3, que p é soma de dois quadrados. Suponhamos a existência de duas representações distintas para p, isto é, $p = a^2+b^2 = c^2+d^2$. Sendo p ímpar um dos números a e b é ímpar enquanto o outro é par. É claro que o mesmo se verifica para os números c e d.

Como $a^2+b^2=c^2+d^2$ temos $a^2-c^2=d^2-b^2$ e, portanto, $(a-c)(a+c) = (d-b)(d+b)$. Seja $r = (a-c, d-b)$, logo $a-c = mr$ e $d-b = nr$ onde $(n, m) = 1$. Portanto, $m(a+c) = n(d+b)$. Sendo $(m, n) = 1$, se tomarmos $s = (a+c, d+b)$, concluímos que $a+c = ns$ e $d+b = ms$. Se a e c são ambos pares ou ambos ímpares temos que r e s são pares. Se somente um deles é par, então r e s são ambos ímpares. Neste caso ambos m e n são ímpares.

É fácil ver que

$$\begin{aligned}(r^2+s^2)(m^2+n^2) &= m^2r^2+m^2s^2+n^2r^2+n^2s^2\\ &= (a-c)^2+(d+b)^2+(d-b)^2+(a+c)^2\\ &= 2(a^2+b^2)+2(c^2+d^2).\end{aligned}$$

Dividindo, membro a membro, por 4 obtemos:

$$\frac{(r^2+s^2)(m^2+n^2)}{4} = \frac{a^2+b^2}{2} + \frac{c^2+d^2}{2} = p.$$

Esta última igualdade nos diz que se r e s são pares então p é o produto dos inteiros $(m^2+n^2)/2$ e $(r^2+s^2)/2$ os quais são maiores do que 1. Se r e s são

ímpares eles não podem ser ambos iguais a 1 pois teríamos, neste caso, $a = d$ e $b = c$. A hipótese de $m = n = 1$ também nos daria $a = d$ e $b = c$. Portanto, quando r e s são ímpares, p é o produto de $(r^2+s^2)/2$ e $(m^2+n^2)/2$ os quais são, ambos, diferentes de 1. Como as duas fatorações acima são impossíveis, uma vez que p é primo, a representação de $p(p \equiv 1(\text{mod } 4))$ como soma de quadrados é única. □

7.5 Problemas Resolvidos

Problema 5.1 Provar que nenhum inteiro da forma $8k+7$ pode ser expresso como a soma de três quadrados.

Solução. É fácil a verificação de que para qualquer inteiro n temos que $n^2 \equiv 0, 1$ ou $4(\text{mod } 8)$. Como a soma de quaisquer três números congruentes a $0, 1$ ou $4(\text{mod } 8)$ nunca é congruente a 7 módulo 8 o resultado segue.

Problema 5.2 Mostre que nenhum inteiro da forma $4^n(8k+7)$ pode ser expresso como a soma de três quadrados.

Solução. Como $m^2 \equiv 0$ ou $1(\text{mod } 4)$ para todo inteiro m, $x^2+y^2+z^2$ poderia ter a forma $4^n(8k+7)$ somente se x, y e z fossem pares. Logo x, y e z poderiam ser divididos por 2 e portanto, $4^{n-1}(8k+7)$ teria, também, uma representação como soma de três quadrados. Mas isto, não pode ocorrer pois implicaria, por repetição deste argumento, na existência de uma tal representação para $8k+7$, a qual não existe pelo Problema 5.1.

Problema 5.3 Representar 765 como soma de dois quadrados.

Solução. Como a fatoração $765 = 3^2 \times 5 \times 17$ não possui nenhuma potência ímpar de primo congruente a 3 módulo 4 o Teorema 7.2 nos garante a existência de uma tal representação. Para encontrar dois quadrados com soma 765 representamos $3^2, 5$ e 17 como soma de dois quadrados e utilizamos a equação (7.2)

$$\begin{aligned}3^2 &= 3^2+0^2\\ 5 &= 1^2+2^2\\ 17 &= 1^2+4^2\\ 765 &= 3^2\times 5\times 17\\ &= (3^2+0^2)(1^2+2^2)(1^2+4^2)\\ &= (3^2+6^2)(1^2+4^2)\\ &= 27^2+6^2.\end{aligned}$$

7.6 Problemas Propostos

1. Dizer quais dentre os primos 11, 17, 19, 23, 29 e 31 possuem representação como soma de dois quadrados e fornecer a representação.

2. Resolver, em inteiros, as seguintes equações $x^2 + y^2 = 146, x^2 + y^2 = 625$.

3. Dizer se existe um triângulo retângulo isósceles de lados inteiros.

4. Mostrar que se o primo p é tal que $p \equiv 3 (\text{mod } 4)$, então a equação $p^2 = a^2 + b^2$ possui solução inteira.

5. Mostrar que, no problema anterior, $a = 0$ ou $b = 0$.

6. Encontrar um inteiro n e racionais, não inteiros, r e s tais que $n = r^2 + s^2$.

7. Mostrar que todo quadrado perfeito pode ser representado como soma dos quadrados de racionais, não-inteiros, r e s.

Capítulo 8

Frações Contínuas

8.1 Definição – Notação

No primeiro capítulo, descrevemos um método que se encontra em *Os Elementos de Euclides*, para se encontrar o máximo divisor comum de dois números.

Basicamente, como veremos a seguir, este método é usado para se converter uma fração em fração contínua. Iniciamos, pois, com um exemplo. Vamos encontrar o máximo divisor comum de 79 e 28 pelo processo das divisões sucessivas.

$$\begin{array}{rcrcr} 79 & = & 2 \times 28 & + & 23 \\ 28 & = & 1 \times 23 & + & 5 \\ 23 & = & 4 \times 5 & + & 3 \\ 5 & = & 1 \times 3 & + & 2 \\ 3 & = & 1 \times 2 & + & 1 \\ 2 & = & 2 \times 1 & + & 0 \end{array}$$

Logo, $(79, 28) = 1$, uma vez que 1 é o último resto não-nulo nesta seqüência de divisões sucessivas.

Como conseqüência imediata destas igualdades, podemos expressar o número racional $79/28$ da seguinte forma:

$$\begin{aligned} \frac{79}{28} &= 2 + \frac{23}{28} = 2 + \frac{1}{\frac{28}{23}} \\ &= 2 + \frac{1}{1 + \frac{5}{23}} = 2 + \frac{1}{1 + \frac{1}{\frac{23}{5}}} = 2 + \frac{1}{1 + \frac{1}{4 + \frac{3}{5}}} \\ &= 2 + \frac{1}{1 + \frac{1}{4 + \frac{1}{\frac{5}{3}}}} = 2 + \frac{1}{1 + \frac{1}{4 + \frac{1}{1 + \frac{2}{3}}}} = \end{aligned}$$

$$= 2 + \cfrac{1}{1 + \cfrac{1}{4 + \cfrac{1}{1 + \cfrac{1}{\frac{3}{2}}}}} = 2 + \cfrac{1}{1 + \cfrac{1}{4 + \cfrac{1}{1 + \cfrac{1}{1 + \frac{1}{2}}}}}$$

Dizemos que esta última expressão é a fração contínua que representa o número racional $79/28$, ou a expressão de $79/28$ sob a forma de fração contínua.

A notação usada é $[2, 1, 4, 1, 1, 2]$. De um modo geral uma expressão da forma

$$a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{a_4 + \cfrac{1}{a_5 + \ddots}}}} \qquad (8.1)$$

é chamada de *fração contínua* e os números $a_1, a_2, \ldots$ são chamados de quocientes parciais. Como vimos acima, na seqüência de divisões sucessivas para a obtenção do máximo divisor comum de 79 e 28, os números a_i são, de fato, quocientes daquelas divisões.

Se o número dos a_i's for finito dizemos que a fração contínua é finita e, caso contrário, dizemos que é infinita.

Quando todos os a_i's são inteiros dizemos que a fração contínua é *simples*. Como vamos nos restringir, apenas, ao caso de frações contínuas simples, a expressão "fração contínua" deverá ser entendida como "fração contínua simples".

Uma expressão como (8.1) será denotada por $[a_1, a_2, a_3, \ldots]$ e $[a_1, a_2, \ldots, a_n]$ é a notação para

$$a_1 + \cfrac{1}{a_2 + \cfrac{}{\ddots + \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}}.$$

Vamos expressar o racional $-37/5$ como uma fração contínua.

É de fácil verificação que,

$$\begin{aligned} -37 &= -8 \times 5 + 3 \\ 5 &= 1 \times 3 + 2 \\ 3 &= 1 \times 2 + 1 \\ 2 &= 2 \times 1 + 0. \end{aligned}$$

Logo,

$$\begin{aligned} \frac{-37}{5} &= -8 + \frac{3}{5} = -8 + \cfrac{1}{\frac{5}{3}} = -8 + \cfrac{1}{1 + \frac{2}{3}} \\ &= -8 + \cfrac{1}{1 + \cfrac{1}{\frac{3}{2}}} = -8 + \cfrac{1}{1 + \cfrac{1}{1 + \frac{1}{2}}} \end{aligned}$$

e, portanto, $-37/5 = [-8, 1, 1, 2]$.

Como se pode ver, no processo de divisões sucessivas, somente o primeiro quociente pode ser negativo. Disto concluímos que na fração contínua *simples* $[a_1, a_2, \ldots]$ todos os a_i's são inteiros positivos, com a possível exceção de a_1.

Vamos considerar a seqüência 2, 1, 4, 5, 3 e a fração contínua representada por $[2, 1, 4, 5, 3]$, i.e.,

$$2 + \cfrac{1}{1 + \cfrac{1}{4 + \cfrac{1}{5 + \frac{1}{3}}}}$$

que pode ser, facilmente, reduzida a

$$2 + \cfrac{1}{1 + \cfrac{1}{4 + \cfrac{1}{\frac{15+1}{3}}}} = 2 + \cfrac{1}{1 + \cfrac{1}{4 + \frac{3}{16}}} = 2 + \cfrac{1}{1 + \cfrac{1}{\frac{64+3}{16}}} =$$

$$= 2 + \frac{67}{83} = \frac{233}{83}$$

É óbvio que toda fração contínua (simples) finita $[a_1, a_2, \ldots, a_n]$ representa um número racional.

A recíproca também é verdadeira, isto é, um número racional pode ser representado sob a forma de fração contínua pois o processo de divisões sucessivas, como vimos no Capítulo 1, sempre, após um número finito de passos (divisões) nos fornece resto nulo.

O número de quocientes parciais a_i, na representação de um número racional pode ser par ou ímpar uma vez que quando o a_n é maior do que 1 podemos substituí-lo por $a_n - 1 + \frac{1}{1}$. Na representação acima de $233/83$ teríamos

$$2 + \cfrac{1}{1 + \cfrac{1}{4 + \cfrac{1}{5 + \frac{1}{3}}}} = 2 + \cfrac{1}{1 + \cfrac{1}{4 + \cfrac{1}{5 + \cfrac{1}{2 + \frac{1}{1}}}}}$$

e, portanto, $[2,1,4,5,3] = [2,1,4,5,2,1]$.

De modo geral, se $a_n > 1$, temos

$$[a_1, a_2, \ldots, a_n] = [a_1, a_2, \ldots, a_n - 1, 1].$$

As observações que acabamos de fazer podem ser resumidas no seguinte teorema.

Teorema 8.1 *Todo número racional pode ser representado de duas maneiras distintas sob a forma de fração contínua e toda fração contínua (simples) finita representa um número racional.*

Chamamos a atenção do leitor para o fato de que a unicidade da representação de um número racional em fração contínua (a menos da modificação do último termo a_n) é garantida pelo Teorema 1.2.

A representação de 19/11 em fração contínua é dada por [1,1,2,1,2] e como

$$\frac{11}{19} = 0 + \frac{1}{\frac{19}{11}} = 0 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \frac{1}{2}}}}}$$

temos que $11/19 = [0,1,1,2,1,2]$.

Na realidade temos, em geral, que se a representação em fração contínua do racional $\frac{p}{q} (p > q)$ é dada por $[a_1, a_2, \ldots, a_n]$, então a representação de $\frac{q}{p}$ é dada por $[0, a_1, a_2, \ldots, a_n]$.

Isto é conseqüência imediata do fato de

$$\frac{q}{p} = 0 + \frac{1}{\frac{p}{q}}.$$

8.2 Convergentes

Vimos que qualquer número racional pode ser representado sob a forma de uma fração contínua (simples)

$$\frac{p}{q} = [a_1, a_2, \ldots, a_{n-1}, a_n]$$

onde a_1 é um inteiro positivo, negativo ou zero, e $a_2, a_3, \ldots, a_n$ são inteiros positivos.

Consideremos as frações

$$c_1 = \frac{a_1}{1},\ c_2 = a_1 + \frac{1}{a_2},\ c_3 = a_1 + \cfrac{1}{a_2 + \frac{1}{a_3}}, \ldots$$

obtidos pelas expansões das frações contínuas

$$[a_1], [a_1, a_2], [a_1, a_2, a_3], \ldots$$

Estas frações são chamadas de primeiro, segundo, terceiro, ... *convergentes*, respectivamente, da fração contínua $[a_1, a_2, a_3, \ldots, a_{n-1}, a_n]$.

É claro que o n-ésimo convergente é igual à própria fração contínua. Nos teoremas seguintes mostramos algumas propriedades satisfeitas pelos convergentes de uma fração contínua.

Se considerarmos

$$c_1 = \frac{a_1}{1} = \frac{p_1}{q_1} \qquad \text{onde} \qquad p_1 = a_1 \quad \text{e} \quad q_1 = 1$$

teremos,

$$c_2 = a_1 + \frac{1}{a_2} = \frac{a_1 a_2 + 1}{a_2} = \frac{p_2}{q_2}$$

onde $p_2 = a_1 a_2 + 1$ e $q_2 = a_2$.

Se calcularmos c_3, c_4, c_5, obtemos, respectivamente:

$$c_3 = \frac{a_3 p_2 + p_1}{a_3 q_2 + q_1} = \frac{p_3}{q_3}$$
$$c_4 = \frac{a_4 p_3 + p_2}{a_4 q_3 + q_2} = \frac{p_4}{q_4}$$
$$c_5 = \frac{a_5 p_4 + p_3}{a_5 q_4 + q_3} = \frac{p_5}{q_5}$$

Observando estes resultados podemos conjectuar que os numeradores p_i's e os denominadores q_i's dos convergentes c_i's satisfazem as seguintes relações:

$$p_i = a_i p_{i-1} + p_{i-2}$$
$$q_i = a_i q_{i-1} + q_{i-2}.$$

No teorema abaixo provamos, por indução, que estas relações se verificam para $i = 3, 4, 5, \ldots, n$.

Teorema 8.2 *Seja $c_i = p_i/q_i$ o i-ésimo convergente da fração contínua $[a_1, a_2, \ldots, a_n]$. Então o numerador p_i e o denominador q_i de c_i satisfazem as seguintes relações:*

$$p_i = a_i p_{i-1} + p_{i-2} \qquad (8.2)$$
$$q_i = a_i q_{i-1} + q_{i-2}$$

para $i = 3, 4, 5, \ldots, n$; *onde*

$$p_1 = a_1, \ p_2 = a_2a_1 + 1, \ q_1 = 1, \ q_2 = a_2.$$

Demonstração: Como já vimos o teorema é válido para $i = 3$, i.e.,

$$c_3 = \frac{p_3}{q_3} = \frac{a_3p_2 + p_1}{a_3q_2 + q_1}.$$

Assumimos, agora, que a relação (8.2) se verifica para todo $j \leq i$ com $3 \leq i < n$. Isto significa que

$$c_i = [a_1, a_2, \ldots, a_i] = \frac{p_i}{q_i} = \frac{a_ip_{i-1} + p_{i-2}}{a_iq_{i-1} + q_{i-2}} \tag{8.3}$$

Observando que,

$$c_i = a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{\ddots}{+\cfrac{1}{a_{i-1} + \cfrac{1}{a_i}}}}}$$

e que,

$$c_{i+1} = a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{\ddots}{+\cfrac{1}{a_{i-1} + \cfrac{1}{a_i + \cfrac{1}{a_{i+1}}}}}}}$$

vemos que c_{i+1} pode ser obtido de c_i simplesmente pela substituição de a_i por $a_i + \frac{1}{a_{i+1}}$. Isto nos diz que se pudermos mostrar que os números $p_{i-1}, p_{i-2}, q_{i-1}$ e q_{i-2} dependem somente dos quocientes parciais $a_1, a_2, \ldots, a_{i-1}$, poderemos usar (8.3) para a obtenção de c_{i+1} pois estamos assumindo, como hipótese de indução, a validade de (8.3) para todo $j \leq i$. Como

$$\frac{p_{i-1}}{q_{i-1}} = \frac{a_{i-1}p_{i-2} + p_{i-3}}{a_{i-1}q_{i-2} + q_{i-3}}$$

os números p_{i-1} e q_{i-1} dependem somente dos números a_{i-1} e dos números $p_{i-2}, q_{i-2}, p_{i-3}, q_{i-3}$ os quais dependem dos precedentes a's, p's e q's. Desta

forma $p_{i-2}, q_{i-2}, p_{i-1}$ e q_{i-1} dependem somente dos primeiros $i-1$ quocientes parciais $a_1, a_2, \ldots, a_{i-1}$ sendo independentes de a_i. Portanto eles não serão alterados com a substituição de a_i por $a_i + \frac{1}{a_{i+1}}$. Podemos, portanto, utilizar (8.3) para a obtenção de c_{i+1} bastando, para isto, substituir a_i por $a_i + \frac{1}{a_{i+1}}$:

$$\begin{aligned}
c_{i+1} &= \frac{\left(a_i + \frac{1}{a_{i+1}}\right)p_{i-1} + p_{i-2}}{\left(a_i + \frac{1}{a_{i+1}}\right)q_{i-1} + q_{i-2}} \\
&= \frac{(a_{i+1}a_i + 1)p_{i-1} + a_{i+1}p_{i-2}}{(a_{i+1}a_i + 1)q_{i-1} + a_{i+1}q_{i-2}} \\
&= \frac{a_{i+1}(a_ip_{i-1} + p_{i-2}) + p_{i-1}}{a_{i+1}(a_iq_{i-1} + q_{i-2}) + q_{i-1}} \\
&= \frac{a_{i+1}p_i + p_{i-1}}{a_{i+1}q_i + q_{i-1}} \\
&= \frac{p_{i+1}}{q_{i+1}}
\end{aligned}$$

o que conclui a demonstração por indução. □

Por uma questão de conveniência vamos definir $p_0 = 1, \ p_{-1} = 0, \ q_0 = 0, \ q_{-1} = 1$. Com estas definições as equações (8.2)

$$\begin{aligned}
p_i &= a_ip_{i-1} + p_{i-2} \\
q_i &= a_iq_{i-1} + q_{i-2}
\end{aligned}$$

passam a ser verdadeiras para todo $i = 1, 2, 3, \ldots$.

A relação obtida no próximo teorema nos permitirá deduzir, facilmente, que para todo convergente $c_i = p_i/q_i$ temos que $(p_i, q_i) = 1$.

Teorema 8.3. *A relação*

$$p_iq_{i-1} - p_{i-1}q_i = (-1)^i \tag{8.4}$$

se verifica para todo $i \geq 0$, *onde* p_i *e* q_i *são, respectivamente, o numerador e o denominador do* i*-ésimo convergente.*

Demonstração: Para $i = 0$ temos $p_0q_{-1} - p_{-1}q_0 = 1 = (-1)^0$ uma vez que $p_0 = q_{-1} = 1$ e $p_{-1} = q_0 = 0$.

Vamos assumir, como hipótese de indução, a validade de (8.4) e mostrar que a mesma relação também se verifica quando substituímos i por $i + 1$.

Sabemos, do teorema anterior, que

$$p_{i+1} = a_{i+1}p_i + p_{i-1} \qquad \text{e} \qquad q_{i+1} = a_{i+1}q_i + q_{i-1}.$$

Logo,

$$\begin{aligned} p_{i+1}q_i - p_iq_{i+1} &= (a_{i+1}p_i + p_{i-1})q_i - p_i(a_{i+1}q_i + q_{i-1}) \\ &= a_{i+1}p_iq_i + p_{i-1}q_i - a_{i+1}p_iq_i - p_iq_{i-1} \\ &= (-1)(p_iq_{i-1} - p_{i-1}q_i) \end{aligned}$$

Utilizando, pois, a hipótese de indução, obtemos

$$p_{i+1}q_i - p_iq_{i+1} = (-1)(-1)^i = (-1)^{i+1}$$

o que conclui a demonstração. □

Corolário 8.4: *Para todo convergente* $c_i = \dfrac{p_i}{q_i}$ *temos que* $(p_i, q_i) = 1$.

Demonstração: Pelo teorema temos que $p_iq_{i-1} - p_{i-1}q_i = (-1)^i$. Isto nos diz que qualquer divisor comum de p_i e q_i deve ser um divisor de 1 ou -1. Logo o máximo divisor comum de p_i e q_i deve ser igual a 1. □

8.3 Aproximações Sucessivas

Nesta seção descrevemos um processo de obtenção de aproximações sucessivas, por racionais, para um número irracional.

Seja α um irracional e seja $a_1 = \lfloor \alpha \rfloor$, isto é, a_1 é o maior inteiro menor do que α. Logo,

$$\alpha = a_1 + \frac{1}{x_1},$$

e, claramente, $x_1 = \dfrac{1}{\alpha - a_1}$ é irracional e $x_1 > 1$. Podemos, pois, escrever x_1 na forma

$$x_1 = a_2 + \frac{1}{x_2}$$

onde $a_2 = \lfloor x_1 \rfloor$, x_2 irracional e $x_2 > 1$. Podemos repetir este processo, obtendo:

$$\alpha = a_1 + \frac{1}{x_1}$$

$$\begin{aligned} x_1 &= a_2 + \frac{1}{x_2} \\ x_2 &= a_3 + \frac{1}{x_3} \\ &\vdots \\ x_n &= a_{n+1} + \frac{1}{x_{n+1}} \end{aligned} \tag{8.5}$$

onde todos os a_i's $(i > 1)$ são inteiros maiores ou iguais a 1 e todos os x_i's são irracionais maiores do que 1. O fato de cada x_i ser irracional nos garante que este processo pode ser repetido um número qualquer de vezes. Utilizando as equações (8.5) vemos que

$$\begin{aligned} \alpha &= a_1 + \frac{1}{x_1} = a_1 + \frac{1}{a_2 + \frac{1}{x_2}} = a_1 + \frac{1}{a_2 + \frac{1}{a_3} + \frac{1}{x_3}} \\ &= a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{a_4 + \frac{1}{x_4}}}}. \end{aligned}$$

Definimos $[a_1, a_2, a_3, \ldots] = \lim_{n\to\infty} [a_1, a_2, \ldots, a_n]$.

Vamos ilustrar este processo obtendo a expansão de $\sqrt{3}$.

Sendo $a_1 = \lfloor \sqrt{3} \rfloor = 1$ e

$$\sqrt{3} = a_1 + \frac{1}{x_1} = 1 + \frac{1}{x_1}$$

temos

$$x_1 = \frac{1}{\sqrt{3}-1} = \frac{1}{(\sqrt{3}-1)}\frac{(\sqrt{3}+1)}{(\sqrt{3}+1)} = \frac{\sqrt{3}+1}{2}.$$

Conseqüentemente

$$\sqrt{3} = 1 + \frac{1}{x_1} = 1 + \frac{1}{\frac{\sqrt{3}+1}{2}}.$$

Como $a_2 = \lfloor \frac{\sqrt{3}+1}{2} \rfloor = 1$ temos

$$\frac{\sqrt{3}+1}{2} = 1 + \frac{1}{x_2}$$

donde obtemos

$$x_2 = \frac{1}{\frac{\sqrt{3}+1}{2} - 1} = \sqrt{3} + 1.$$

Logo,

$$\begin{aligned}\sqrt{3} &= 1 + \frac{1}{x_1} = 1 + \frac{1}{1 + \frac{1}{x_2}} = \\ &= 1 + \frac{1}{1 + \frac{1}{\sqrt{3}+1}}\end{aligned}$$

Como $a_3 = \lfloor \sqrt{3} + 1 \rfloor = 2$, temos

$$\sqrt{3} + 1 = x_2 = a_3 + \frac{1}{x_3} = 2 + \frac{1}{x_3}.$$

Resolvendo esta última equação para x_3 obtemos:

$$x_3 = \frac{1}{(\sqrt{3} + 1 - 2)} = \frac{\sqrt{3}+1}{2}$$

Sendo $x_3 = x_1$ concluímos que x_4 será igual a x_2 e desta forma, continuando com este processo, iremos obter para a seqüência $a_1, a_2, a_3, \ldots$ os valores 1,1,2,1, 2,1,2,.... Logo a fração contínua infinita representando $\sqrt{3}$ será dada por:

$$\sqrt{3} = [1, 1, 2, 1, 2, 1, 2, \ldots] = [1, \overline{1, 2}]$$

Chamamos *fração contínua periódica* a uma representação como esta em que uma seqüência de números se repete periodicamente. Colocamos uma barra sobre a parte que se repete que é chamada de *período* da fração contínua.

Para $\alpha = \sqrt{6}$ obtemos a seguinte seqüência

$$\begin{aligned}a_1 &= \lfloor \sqrt{6} \rfloor = 2 \\ x_1 &= \frac{1}{\sqrt{6} - 2} = \frac{\sqrt{6}+2}{2} \\ a_2 &= \left\lfloor \frac{\sqrt{6}+2}{2} \right\rfloor = 2 \\ x_2 &= \frac{1}{\left(\frac{\sqrt{6}+2}{2}\right) - 2} = \sqrt{6} + 2\end{aligned}$$

$$\begin{aligned}a_3 &= \lfloor \sqrt{6} + 2 \rfloor = 4 \\ x_3 &= \frac{1}{(\sqrt{6}+2) - 4} = \frac{\sqrt{6}+2}{2} = x_1\end{aligned}$$

Como $x_3 = x_1$, vemos que $a_4 = a_2, a_5 = a_3, a_6 = a_2, a_7 = a_3, \ldots$. Logo,

$$\sqrt{6} = [2, 2, 4, 2, 4, \ldots] = [2, \overline{2, 4}].$$

Dada uma fração contínua periódica podemos reverter o processo acima para a obtenção do número irracional representado por ela.

Consideremos

$$\begin{aligned}[2, \overline{2, 4}] &= 2 + \cfrac{1}{2 + \cfrac{1}{4 + \cfrac{1}{2 + \cfrac{1}{4 + \ddots}}}} \\ &= 2 + \frac{1}{y}\end{aligned}$$

onde

$$y = 2 + \cfrac{1}{4 + \cfrac{1}{2 + \cfrac{1}{4 + \cfrac{1}{2 + \cfrac{1}{4 + \ddots}}}}}$$

Desta última igualdade observamos que,

$$y = 2 + \frac{1}{4 + \frac{1}{y}}$$

da qual obtemos a equação $2y^2 - 4y - 1 = 0$, ou seja, $y = \dfrac{2+\sqrt{6}}{2}$, uma vez que y é positivo. Logo,

$$\begin{aligned}[2, \overline{2, 4}] &= 2 + \frac{1}{y} = 2 + \frac{1}{\left(\frac{2+\sqrt{6}}{2}\right)} \\ &= 2 + \frac{2}{2+\sqrt{6}} = 2 + \frac{2(2-\sqrt{6})}{-2} \\ &= \frac{-4 + 4 - 2\sqrt{6}}{-2} = \sqrt{6}.\end{aligned}$$

Até o presente momento já vimos que toda fração contínua finita representa um racional, que todo racional é representado por uma fração contínua finita e que um irracional é representado por uma fração contínua infinita.

Vale mencionar que nem todo irracional possui uma representação periódica quando representado sob a forma de fração contínua. O número π possui a seguinte representação

$$\pi = [3, 7, 15, 1, 292, 1, 1, 1, 2, 1, 3, \dots]$$

onde não há nenhuma seqüência (período) que se repete. Lagrange , em 1770, caracterizou todos os irracionais que possuem representação periódica quando expressos sob a forma de fração contínua. Ele mostrou que a fração contínua infinita que representa um irracional é periódica se, e somente se, este irracional for raiz de um polinômio da forma $ax^2 + bx + c = 0$ onde a, b e c são inteiros. Este resultado nos diz, em particular, que somente irracionais algébricos podem ter representação periódica.

8.4 Propriedades dos Convergentes

No teorema seguinte mostramos algumas importantes propriedades da seqüência $c_1, c_2, c_3, \dots$ dos convergentes de uma fração contínua.

Teorema 8.5 *A seqüência $c_1, c_2, c_3, \dots$ dos convergentes de uma fração contínua satisfaz as seguintes propriedades:*

(i) $c_1 < c_3 < c_5 < c_7 < \cdots < c_{2n+1}$

(ii) $c_2 > c_4 > c_6 > \cdots > c_{2n}$

(iii) $c_{2n+1} < c_{2n+2} < c_{2n}$.

Demonstração: Pelo Teorema 8.3 temos que

$$p_i q_{i-1} - p_{i-1} q_i = (-1)^i \tag{8.6}$$

a qual é válida independentemente da fração contínua ser finita ou não. Dividindo ambos os lados desta igualdade por $q_i q_{i-1}$ obtemos:

$$\frac{p_i}{q_i} - \frac{p_{i-1}}{q_{i-1}} = \frac{(-1)^i}{q_i q_{i-1}}$$

Como $c_i = \dfrac{p_i}{q_i}$ temos que

$$c_i - c_{i-1} = \frac{(-1)^i}{q_i q_{i-1}} \tag{8.7}$$

Mas sendo

$$c_i - c_{i-2} = \frac{p_i}{q_i} - \frac{p_{i-2}}{q_{i-2}} = \frac{p_i q_{i-2} - p_{i-2} q_i}{q_i q_{i-2}} \tag{8.8}$$

obtemos, usando o fato de $p_i = a_i p_{i-1} + p_{i-2}$ e $q_i = a_i q_{i-1} + q_{i-2}$, que

$$\begin{aligned} c_i - c_{i-2} &= \frac{(a_i p_{i-1} + p_{i-2}) q_{i-2} - p_{i-2}(a_i q_{i-1} + q_{i-2})}{q_i q_{i-2}} \\ &= \frac{a_i (p_{i-1} q_{i-2} - p_{i-2} q_{i-1})}{q_i q_{i-2}} \\ &= \frac{a_i (-1)^{i-1}}{q_i q_{i-2}} \end{aligned}$$

isto é,

$$c_i - c_{i-2} = \frac{a_i (-1)^{i-1}}{q_i q_{i-2}} \tag{8.9}$$

Tomando $i = 2$ e $i = 3$ em (8.7) obtemos, respectivamente,

$$c_2 - c_1 = \frac{1}{q_2 q_1} > 0 \qquad \text{e} \qquad c_3 - c_2 = \frac{-1}{q_3 q_2} < 0$$

uma vez que todos os q_i's são positivos.

A equação (8.9) nos diz que para $i = 3$ temos

$$c_3 - c_1 = \frac{a_3}{q_3 q_1} > 0$$

pois a_3, q_3 e q_1 são, todos, positivos. Sendo, pois, $c_1 < c_3, c_1 < c_2$ e $c_2 > c_3$ temos que $c_1 < c_3 < c_2$. Usando, agora, $i = 3$ e $i = 4$ em (8.7) e $i = 4$ em (8.9) obtemos $c_3 < c_4 < c_2$. Repetindo este processo obtemos a seqüência de desigualdades:

$$\begin{gathered} c_5 < c_6 < c_4 \\ c_7 < c_8 < c_6 \\ \vdots \end{gathered}$$

Combinando estas desigualdades obtemos

$$c_1 < c_3 < c_5 < c_7 < \cdots < c_{2i+1} < \cdots < c_{2n} < \cdots < c_6 < c_4 < c_2$$

o que conclui a demonstração. □

O que acabamos de mostrar é que a seqüência dos convergentes de índice ímpar forma uma seqüência crescente que é limitada superiormente e que a seqüência dos convergentes de índice par forma uma seqüência decrescente e limitada inferiormente.

Há um resultado fundamental em Análise que diz que toda seqüência crescente e limitada superiormente converge e que toda seqüência decrescente e limitada inferiormente também converge.

Sejam, pois, ℓ_I o limite da seqüência $c_1, c_3, c_5, \ldots, c_{2i+1}, \ldots$ e ℓ_P o limite da seqüência $c_2, c_4, c_6, \ldots, c_{2i}, \ldots$.

Como os números q_i's são calculados através da relação $q_i = a_i q_{i-1} + q_{i-2}$ e os números $a_i (i \geq 2)$ e $q_i (i \geq 1)$ são todos positivos concluímos que a seqüência dos q_i's cresce indefinidamente. Isto implica que se tomarmos $i = 2j$ em (8.7), teremos

$$c_{2j} - c_{2j-1} = \frac{1}{q_{2j} q_{2j-1}}$$

o que nos permite concluir que o $\lim\limits_{j \to \infty} (c_{2j} - c_{2j-1}) = 0$.

Sendo $\lim\limits_{j \to \infty} c_{2j-1} = \ell_I$ e $\lim\limits_{j \to \infty} c_{2j} = \ell_P$ concluimos que $\ell_p = \ell_I$.

Mencionamos, anteriormente, a possibilidade de se obter um processo de aproximações sucessivas, por racionais, para um número irracional. Já vimos como obter a representação sob a forma de fração contínua para um irracional e, também, que a seqüência $c_1, c_2, c_3, \ldots$ dos convergentes de uma fração contínua converge.

Provamos, a seguir, que o limite ℓ para o qual a seqüência dos convergentes converge é, na realidade, o número irracional que deu origem à fração contínua. Embora este fato pareça óbvio ele precisa ser provado. Para isto necessitamos do seguinte resultado.

Teorema 8.6 *Para qualquer número real α temos:*

$$[a_1, a_2, \ldots, a_{i-1}, \alpha] = \frac{\alpha p_{i-1} + p_{i-2}}{\alpha q_{i-1} + q_{i-2}} \tag{8.10}$$

onde $a_1, a_2, a_3, \ldots$ é uma seqüência infinita de inteiros positivos com a possível exceção de a_1 e as seqüências dos p_i's e q_i's são dadas por (8.2), isto é,

$$\begin{aligned} p_0 &= 1, p_{-1} = 0, \ q_0 = 0, \ q_{-1} = 1 \\ p_i &= a_i p_{i-1} + p_{i-2} \\ q_i &= a_i q_{i-1} + q_{i-2}, \ i \geq 1. \end{aligned}$$

Demonstração: Para $n = 1$ o resultado deve ser visto como

$$\alpha = \frac{\alpha p_0 - p_{-1}}{\alpha q_0 + q_{-1}}$$

o qual é verdadeiro pelas condições iniciais.

Para $n = 2$ temos

$$[a_1, \alpha] = \frac{\alpha p_1 + p_0}{\alpha q_1 + q_0} = \frac{\alpha a_1 + 1}{\alpha}$$

o que é verdadeiro uma vez que $[a_1, \alpha] = a_1 + \frac{1}{\alpha}$.

Estabelecemos, agora, o resultado por indução. Considerando verdadeiro o resultado para $[a_1, a_2, \ldots, a_{i-1}, \alpha]$ temos

$$\begin{aligned} [a_1, a_2, \ldots, a_i, \alpha] &= [a_1, a_2, \ldots, a_{i-1}, a_i + \frac{1}{\alpha}] \\ &= \frac{(a_i + \frac{1}{\alpha}) p_{i-1} + p_{i-2}}{(a_i + \frac{1}{\alpha}) q_{i-1} + q_{i-2}} \\ &= \frac{\alpha(a_i p_{i-1} + p_{i-2}) + p_{i-1}}{\alpha(a_i q_{i-1} + q_{i-2}) + q_{i-1}} \\ &= \frac{\alpha p_i + p_{i-1}}{\alpha q_i + q_{i-1}} \end{aligned}$$

o que prova (8.10). □

Consideramos, agora, a seqüência $a_1, a_2, a_3, \ldots$ dada por (8.5) e a seqüência dos convergentes $c_i = p_i / q_i$. Sabemos que,

$$\begin{aligned} \alpha &= a_1 + \frac{1}{x_1} = [a_1, x_1] = [a_1, a_2 + \frac{1}{x_2}] \\ &= [a_1, a_2, x_2] = [a_1, a_2, a_3 + \frac{1}{x_3}] = \\ &= [a_1, a_2, a_3, x_3] = [a_1, a_2, \ldots, a_{i-1} + \frac{1}{x_{i-1}}] \\ &= [a_1, a_2, a_3, \ldots, a_{i-1}, x_{i-1}] \end{aligned}$$

e pelo Teorema 8.6 temos

$$\alpha = [a_1, a_2, a_3, \ldots, a_{i-1}, x_{i-1}] = \frac{x_{i-1} p_{i-1} + p_{i-2}}{x_{i-1} q_{i-1} + q_{i-2}}.$$

Tomando a diferença

$$\alpha - c_{i-1} = \frac{x_{i-1} p_{i-1} + p_{i-2}}{x_{i-1} q_{i-1} + q_{i-2}} - \frac{p_{i-1}}{q_{i-1}}$$

$$= \frac{-(p_{i-1}q_{i-2} - p_{i-2}q_{i-1})}{q_{i-1}(x_{i-1}q_{i-1} + q_{i-2})} \qquad (8.11)$$

$$\overset{(8.6)}{=} \frac{(-1)^i}{q_{i-1}(x_{i-1}q_{i-1} + q_{i-2})}$$

podemos concluir que $\lim_{i\to\infty}(\alpha - c_{i-1}) = 0$ uma vez que a seqüência dos q_i's é crescente e os números x_i's são positivos.

Portanto $\alpha = \lim_{i\to\infty} c_i = \lim_{i\to\infty}[a_1, a_2, \ldots, a_i] = [a_1, a_2, a_3, \ldots]$, ou seja, o limite da seqüência dos convergentes da representação do irracional α sob a forma de fração contínua é igual ao próprio α.

O Teorema 8.5 nos permite provar que toda fração contínua simples infinita representa um irracional. Isto é o que mostramos no próximo teorema.

Teorema 8.7 *Toda fração contínua simples infinita* $[a_1, a_2, a_3, \ldots]$ *representa um irracional.*

Demonstração: Denotando $[a_1, a_2, a_3, \ldots]$ por α nós observamos, pelo Teorema 8.5, que α está entre c_i e c_{i+1} e, portanto, $0 < |\alpha - c_i| < |c_{i+1} - c_i|$.

Multiplicando por q_i esta desigualdade e utilizando (8.7) temos

$$0 < |\alpha q_i - p_i| < |c_{i+1}q_i - c_i q_i| < \frac{1}{q_{i+1}}.$$

Supondo α racional, isto é, $\alpha = \frac{a}{b}$, a e b inteiros com $b > 0$, a desigualdade acima, após multiplicação por b nos fornece

$$|aq_i - bp_i| < \frac{b}{q_{i+1}}.$$

Como a seqüência dos q_i é crescente podemos escolher i suficientemente grande de forma que $b < q_{i+1}$.

Desta forma o inteiro $aq_i - bp_i$ estaria entre 0 e 1, o que é impossível. □

Nos próximos teoremas são provados dois importantes resultados. Mostramos que todo convergente $\frac{p_n}{q_n}$ de α satisfaz

$$\left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{q_n^2}$$

e que se o racional a/b, $b > 0$ verificar

$$\left|\alpha - \frac{a}{b}\right| < \frac{1}{2b^2}$$

então a/b é um dos convergentes da representação de α em fração contínua.

Teorema 8.8 *Todo convergente* $c_i = \frac{p_i}{q_i}$ *de* α *satisfaz*

$$\left|\alpha - \frac{p_i}{q_i}\right| < \frac{1}{q_i^2}.$$

Demonstração: Por (8.5) temos que $a_{n+1} < x_n$. Este fato, juntamente com (8.11), nos fornece

$$\left|\alpha - \frac{p_i}{q_i}\right| = \frac{1}{q_i(x_i q_i + q_{i-1})} < \frac{1}{q_i(a_{i+1}q_i + q_{i-1})}.$$

Usando (8.2) substituímos $a_{i+1}q_i + q_{i-1}$ por q_{i+1} obtendo

$$\left|\alpha - \frac{p_i}{q_i}\right| < \frac{1}{q_i q_{i+1}} < \frac{1}{q_i^2}$$

onde usamos o fato de $q_i < q_{i+1}$ uma vez que a seqüência dos q_i's é estritamente crescente. □

Teorema 8.9 *Seja* α *um irracional e* p_n/q_n *os convergentes da expansão de* α *em fração contínua. Se* a/b *for um racional com* $b > 0$ *tal que*

$$\left|\alpha - \frac{a}{b}\right| < \left|\alpha - \frac{p_n}{q_n}\right|$$

para algum $n \geq 1$, *então* $b > q_n$. *Mais ainda, se* $|\alpha b - a| < |\alpha q_n - p_n|$ *para algum* $n \geq 0$, *então* $b \geq q_{n+1}$.

Demonstração: Inicialmente mostramos que a segunda parte do teorema implica a primeira. Supondo falsa a primeira parte teremos a existência de um racional a/b com

$$\left|\alpha - \frac{a}{b}\right| < \left|\alpha - \frac{p_n}{q_n}\right| \qquad \text{e} \qquad b \leq q_n.$$

Destas desigualdades obtemos

$$|\alpha b - a| < |\alpha q_n - p_n|.$$

Mas a segunda parte do teorema nos diz que isto implica $b \geq q_{n+1}$. Logo temos uma contradição pois $q_n < q_{n+1}$ para $n \geq 0$.

Para provarmos a segunda parte procedemos, novamente, por contradição. Suponhamos $|\alpha b - a| < |\alpha q_n - p_n|$ e $b < q_{n+1}$.

Consideremos o sistema linear em x e y

$$\begin{cases} p_n x + p_{n+1} y = a \\ q_n x + q_{n+1} y = b \end{cases} \tag{8.12}$$

Por (8.4) o determinante principal deste sistema é ± 1 e, conseqüentemente, este sistema possui uma solução em inteiros x e y. Na realidade ambos, x e y, são diferentes de zero. Isto porque se $x = 0$ então $b = yq_{n+1}$ o que implica $y > 0$ e $b \geq q_{n+1}$, em contradição com $b < q_{n+1}$.

Se $y = 0$ então $a = xp_n, b = xq_n$ e

$$\begin{aligned} |\alpha b - a| &= |\alpha x q_n - x p_n| \\ &= |x|\,|\alpha q_n - p_n| \geq |\alpha q_n - p_n| \end{aligned}$$

uma vez que $|x| \geq 1$ o que nos dá, novamente, uma contradição.

A seguir mostramos que x e y possuem sinais opostos. Se $y < 0$, então $xq_n = b - yq_{n+1}$, isto é, $x > 0$.

Se $y > 0$ então $b < yq_{n+1}$ pois $b < q_{n+1}$. Portanto xq_n é negativo o que nos diz que $x < 0$.

Concluímos, agora, de (8.11) que $\alpha q_n - p_n$ e $\alpha q_{n+1} - p_{n+1}$ possuem sinais opostos e, portanto, $x(\alpha q_n - p_n)$ e $y(\alpha q_{n+1} - p_{n+1})$ possuem o mesmo sinal.

Do sistema (8.12) obtemos $\alpha b - a = x(\alpha q_n - p_n) + y(\alpha q_{n+1} - p_{n+1})$.

Desta forma, como os dois termos da direita da igualdade acima possuem o mesmo sinal, temos

$$\begin{aligned} |\alpha b - a| &= |x(\alpha q_n - p_n) + y(\alpha q_{n+1} - p_{n+1})| \\ &= |x(\alpha q_n - p_n)| + |y(\alpha q_{n+1} - p_{n+1})| \\ &> |x(\alpha q_n - p_n)| = |x|\,|\alpha q_n - p_n| \\ &\geq |\alpha q_n - p_n|. \end{aligned}$$

Como isto nos dá uma contradição, o teorema está provado. □

Teorema 8.10 (Lagrange) *Seja α um número irracional. Se existir um racional $a/b, b \geq 1$, tal que*

$$\left|\alpha - \frac{a}{b}\right| < \frac{1}{2b^2}$$

então a/b é um dos convergentes da expansão de α em fração contínua.

Demonstração: Suponhamos que exista a/b um racional satisfazendo a hipótese do teorema e que a/b não seja um convergente da fração contínua de α. Sem perda de generalidade podemos supor $(a, b) = 1$. Seja n o inteiro tal que $q_n \leq b < q_{n+1}$. Para este inteiro n a desigualdade $|\alpha b - a| < |\alpha q_n - p_n|$ é impossível pelo Teorema 8.9. Logo

$$|\alpha q_n - p_n| \leq |\alpha b - a| < \frac{1}{2b},$$

$$\left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{2bq_n}.$$

Usando o fato de que $a/b \neq p_n/q_n$ e que $bp_n - aq_n$ é um inteiro não nulo obtemos

$$\begin{aligned} \frac{1}{bq_n} &\leq \frac{|bp_n - aq_n|}{bq_n} = \left|\frac{p_n}{q_n} - \frac{a}{b}\right| \\ &= \left|\alpha - \frac{a}{b} + \frac{p_n}{q_n} - \alpha\right| \\ &\leq \left|\alpha - \frac{a}{b}\right| + \left|\alpha - \frac{p_n}{q_n}\right| \\ &< \frac{1}{2b^2} + \frac{1}{2bq_n} \end{aligned}$$

e isto implica $b < q_n$ o que, sendo uma contradição, completa a prova do teorema. □

8.5 Problemas Resolvidos

Problema 5.1 Mostrar que para $\alpha \in \mathbb{R}$ a seguinte relação se verifica

$$q_n|q_{n-1}\alpha - p_{n-1}| + q_{n-1}|q_n\alpha - p_n| = 1.$$

Solução. Como α está entre p_n/q_n e p_{n-1}/q_{n-1}, temos

$$\left|\alpha - \frac{p_{n-1}}{q_{n-1}}\right| + \left|\alpha - \frac{p_n}{q_n}\right| = \left|\frac{p_{n-1}}{q_{n-1}} - \frac{p_n}{q_n}\right| = 1/q_n q_{n-1}.$$

Basta multiplicar, ambos os membros, por $q_n q_{n-1}$, que o resultado segue.

Problema 5.2 Mostrar que se $a_1 > 0$ e $\frac{p_n}{q_n} = [a_1, a_2, \ldots, a_n]$ então,

$$\frac{p_n}{p_{n-1}} = [a_n, a_{n-1}, \ldots, a_2, a_1]$$

Solução. Para $n = 1$ temos $[a_1] = a_1 = \frac{a_1}{1} = \frac{p_1}{p_0}$. Portanto o resultado é verdadeiro para $n = 1$.

Assumimos que,

$$\frac{p_k}{p_{k-1}} = [a_k, a_{k-1}, \ldots, a_2, a_1]$$

onde $1 \le k < n$. Então,

$$\begin{aligned}[a_{k+1}, a_k, a_{k-1}, \ldots, a_2, a_1] &= a_{k+1} + \frac{1}{[a_k, a_{k-1}, \ldots, a_2, a_1]} \\ &= a_{k+1} + \frac{1}{p_k/p_{k-1}} \\ &= \frac{a_{k+1}p_k + p_{k-1}}{p_k} = \frac{p_{k+1}}{p_k}\end{aligned}$$

pelo Teorema 8.2. Portanto o resultado é verdadeiro por indução.

Problema 5.3 Uma fração contínua simples é chamada simétrica no caso em que $a_i = a_{n-i}$ para $0 \le i \le n$. Por exemplo [3,2,1,2,3] é simétrica. Mostrar que se o racional $r/s, (r,s) = 1$, possui representação simétrica então,

$$r|(s^2 + (-1)^n).$$

Solução. Sendo $(r,s) = 1$ temos que $\frac{r}{s} = \frac{p_n}{q_n} \Rightarrow r = p_n$ e $s = q_n$ uma vez que $(p_n, q_n) = 1$.

Pelo problema anterior e pelo fato de $\frac{r}{s}$ possuir representação simétrica temos que,

$$\begin{aligned}\frac{p_n}{p_{n-1}} &= [a_n, a_{n-1}, \ldots, a_2, a_1] = [a_1, a_2, \ldots, a_n] \\ &= \frac{r}{s}\end{aligned}$$

o que nos diz que $q_n = p_{n-1} = s$.

Como pelo Teorema 8.3 $p_nq_{n-1} - p_{n-1}q_n = (-1)^n$ concluímos que,

$$rq_{n-1} - s^2 = (-1)^n.$$

Logo, $rq_{n-1} = s^2 + (-1)^n$ e, portanto, $r|(s^2 + (-1)^n)$.

8.6 Problemas Propostos

1. Encontrar o número racional representado sob a forma de fração contínua em cada ítem abaixo:

a) [3,1]
b) [1,1,1]
c) [0,6,5]
d) [1,2,3,4]
c) [2,2,2]
f) [3,6,1,7]
g) [3,7,15,1]
h) [2,3,2,1,2]

2. A representação sob a forma de fração contínua simples infinita (não-periódica) do número e é dada por:

$$e = [2, 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, \ldots]$$

Encontrar os primeiros 6 convergentes desta fração contínua.

3. Encontrar o irracional representado pela fração contínua $[1, 1, 1, 1, \ldots]$.

4. Expressar os seguintes racionais sob a forma de fração contínua

a) $11/7$ b) $-51/23$ c) $114/235$ d) $34/21$

5. Mostrar que se $p_n/q_n = [a_1, a_2, \ldots, a_n]$ então $q_n/q_{n-1} = [a_n, a_{n-1}, \ldots, a_3, a_2]$

6. Suponha que $r > s > 0, (r,s) = 1$ e que $\frac{r}{s} = [a_1, a_2, \ldots, a_n]$. Mostrar que se $p_n|(q_n^2 + (-1)^n)$ então $a_i = a_{n-i}$ para $1 \le i < n$, isto é, $[a_1, a_2, \ldots, a_n]$ é simétrica. (sugestão: ver problema resolvido número 3)

Capítulo 9

Partições

9.1 Partições

As partições de um inteiro positivo são as diferentes maneiras de se expressar este inteiro como soma de inteiros positivos. As partições dos inteiros 3, 4, 5 e 6 são as seguintes

3	4	5	6
$2+1$	$3+1$	$4+1$	$5+1$
$1+1+1$	$2+2$	$3+2$	$4+2$
	$2+1+1$	$3+1+1$	$4+1+1$
	$1+1+1+1$	$2+2+1$	$3+3$
		$2+1+1+1$	$3+2+1$
		$1+1+1+1+1$	$3+1+1+1$
			$2+2+2$
			$2+2+1+1$
			$2+1+1+1+1$
			$1+1+1+1+1+1$

Tabela 9.1

Denotamos por $p(n)$ o número de partições de n. Da tabela acima temos que $p(3) = 3$, $p(4) = 5$, $p(5) = 7$ e $p(6) = 11$. Os números que compõem uma partição são chamados de *partes* desta partição. É claro (da definição) que, numa partição de n, nenhuma parte pode superar n, e que a ordem das partes não está sendo considerada. Para ilustrar quão rápido é o crescimento de $p(n)$, listamos alguns outros valores: $p(20) = 627$, $p(100) = 190.569.292$ e $p(200) = 3.972.999.029.388$. Mencionamos, ao leitor interessado, a existência de uma fórmula exata para o cálculo de $p(n)$. Isto resultou do trabalho dos matemáticos S. Ramanujan, G.H. Hardy e H. Rademacher, ver [2]. As principais idéias para a obtenção desta genial fórmula foram do grande matemático indiano Ramanujan.

Se denotarmos por $p_k(n)$ o número de partições de n tendo k como a maior parte, a tabela anterior nos diz que $p_2(3) = 1$, $p_3(5) = 2$, $p_4(5) = 1$, $p_5(6) = 1$ e $p_3(6) = 3$.

Como a maior parte não pode superar n, temos que $p_n(n) = 1$ e $p_k(n) = 0$, para $k > n$.

Listamos a seguir os valores de $p_k(6)$, para $k = 1, 2, \ldots, 6$.

k	1	2	3	4	5	6
$p_k(6)$	1	3	3	2	1	1

Tabela 9.2

É claro que,

$$\sum_{k=1}^{6} p_k(6) = p(6)$$

e, em geral,

$$\sum_{k=1}^{n} p_k(n) = p(n).$$

Podemos também classificar o número de partições de n de acordo com o número de partes. Observando as partições de 6 listadas na Tabela 9.1 e denotando por $q_k(n)$ o número de partições de n com exatamente k partes, temos a tabela abaixo.

k	1	2	3	4	5	6
$q_k(6)$	1	3	3	2	1	1

Tabela 9.3

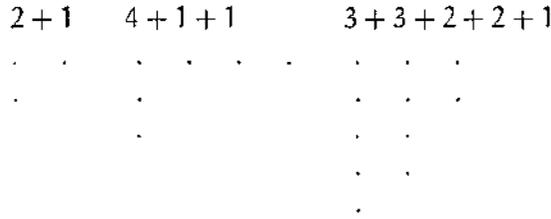
Pode-se observar que os valores listados para $p_k(6)$ e $q_k(6)$, nas Tabelas 9.2 e 9.3, são os mesmos. Não se trata de coincidência. Como mostramos a seguir, $p_k(n) = q_k(n)$, para todo n.

9.2 Gráfico de uma partição

Uma partição do inteiro n pode ser representada graficamente por meio de um conjunto de n pontos no plano, colocando-se em cada linha, e em ordem decrescente, um número de pontos igual a cada uma de suas partes.

O gráfico da partição $4+3+1+1$ de 9 é:

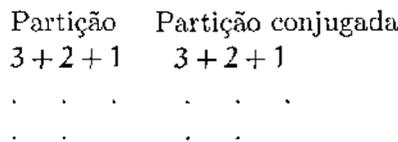
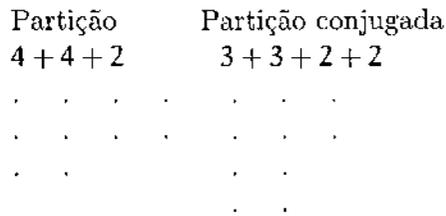
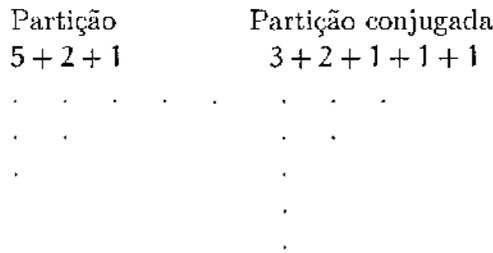
As partições $2+1$, $4+1+1$ e $3+3+2+2+1$ possuem as seguintes representações gráficas:

$2+1$ $\quad$ $4+1+1$ $\quad$ $3+3+2+2+1$

Se na representação gráfica de uma partição de n trocarmos as linhas pelas colunas, obtemos uma outra partição de n chamada de *conjugada* da partição considerada.

Listamos a seguir os gráficos de algumas partições com suas respectivas partições conjugadas.

Partição	Partição conjugada
$5+2+1$	$3+2+1+1+1$

Partição	Partição conjugada
$4+4+2$	$3+3+2+2$

Partição	Partição conjugada
$3+2+1$	$3+2+1$

Observe que a conjugada de uma partição não é, necessariamente, distinta da partição original.

Teorema 9.1 *O número $p_k(n)$ de partições de n tendo k como a maior parte é igual ao número $q_k(n)$ de partições de n com exatamente k partes, isto é, $p_k(n) = q_k(n)$.*

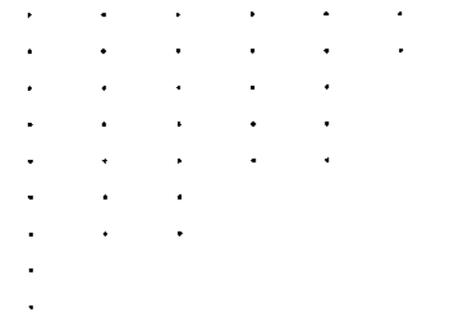
Demonstração: Por intermédio da operação "conjugação" definida no conjunto das partições de n, vemos facilmente que toda partição tendo k como maior parte é transformada em uma partição que posssui exatamente k partes, e que cada uma que possui k partes é levada em uma que possui k como a maior parte, o que conclui a demonstração. □

Corolário 9.2 *Seja $P_k(n)$ o número de partições de n com partes menores do que ou iguais a k, e $Q_k(n)$ o número de partições de n com, no máximo, k partes. Então, $P_k(n) = Q_k(n)$.*

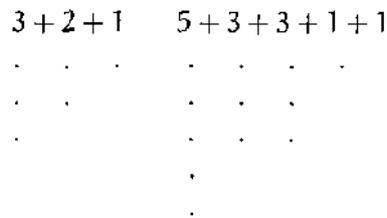
Demonstração: A operação de conjugação transforma cada elemento contado por $P_k(n)$ em um único elemento contado por $Q_k(n)$, isto pela mesma razão apresentada na demonstração do teorema. □

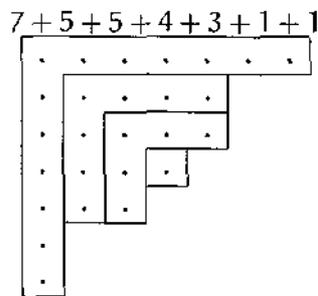
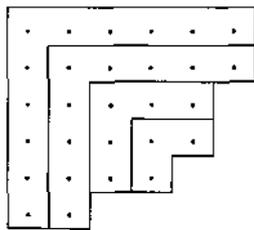
Se denotarmos por $F(n)$ o número de partições de n em que cada parte aparece pelo menos duas vezes e por $G(n)$ o número de partições de n em partes maiores do que 1 e tais que inteiros consecutivos não aparecem como partes, pode-se mostrar que $F(n) = G(n)$.

Teorema 9.3 $F(n) = G(n)$ *para todo inteiro positivo* n.

Demonstração: Uma vez mais tomando-se o conjugado de uma partição enumerada por $F(n)$, teremos exatamente um dos elementos enumerados por $G(n)$. O exemplo abaixo ilustra esta afirmação.

O fato de cada parte aparecer pelo menos duas vezes implica que, na partição conjugada, a menor parte será pelo menos 2 e que inteiros consecutivos não poderão ocorrer como partes. □

Dizemos que uma partição é *autoconjugada* se ela for igual à sua conjugada. Por exemplo, $3+2+1$ e $5+3+3+1+1$ são autoconjugadas, como se pode verificar pelas suas representações gráficas:

$3+2+1$ $\quad$ $5+3+3+1+1$

Se, em cada uma delas, trocarmos as linhas pelas colunas teremos a mesma partição. Uma simples transformação, que daremos a seguir, nos permite provar que o número de partições de n que são autoconjugadas é igual ao número de partições de n em partes ímpares distintas. Para ilustrarmos esta transformação vamos considerar a seguinte partição autoconjugada de 26.

$7+5+5+4+3+1+1$

É claro que o número de pontos dentro de cada uma das áreas delimitadas é ímpar e estes números são necessariamente distintos. Neste caso, temos $13+7+5+1$. Reciprocamente, dados números ímpares distintos, podemos colocá-los numa disposição semelhante a que temos acima, obtendo, desta forma, o gráfico de uma partição autoconjugada. Por exemplo, a partição $11+9+5+3$ de 28 pode ser representada por:

e é, obviamente, autoconjugada. Temos, portanto, demonstrado o teorema:

Teorema 9.4 *O número de partições autoconjugadas de n é igual ao número de partições de n em partes ímpares distintas.*

9.3 Funções Geradoras

Antes de introduzirmos o conceito de função geradora para partições, gostaríamos de chamar a atenção do leitor para uma importante interpretação combinatorial para $q_k(n)$, o número de partições de n com exatamente k partes. Como vimos, as partições de 6 são {6}, {5, 1}, {4, 2}, {4, 1, 1}, {3, 3}, {3, 2, 1}, {3, 1, 1, 1}, {2, 2, 2}, {2, 2, 1, 1}, {2, 1, 1, 1, 1} e {1, 1, 1, 1, 1, 1}.

Se desejarmos distribuir 6 objetos idênticos em 3 caixas idênticas, sem que nenhuma fique vazia, teremos apenas as possibilidades {4, 1, 1}, {3, 2, 1} e {2, 2, 2}, que são as partições de 6 em exatamente 3 partes. De maneira análoga podemos concluir que o número de maneiras de se distribuir n objetos idênticos em k caixas idênticas, sem que nenhuma fique vazia, é igual a $q_k(n)$.

Pretendemos, através de exemplos, introduzir o conceito de função geradora.

Consideremos a função $F(x) = (1+x)^n$. Na sua expansão, i.e.,

$$(1+x)^n = \binom{n}{0} + \binom{n}{1}x + \binom{n}{2}x^2 + \cdots + \binom{n}{n}x^n$$

podemos observar que o coeficiente de x^k é igual a $\binom{n}{k}$.

Diremos, então, que a seqüência $a_k = \binom{n}{k}$ para $k = 0, 1, 2, \ldots, n$ é gerada por $(1+x)^n$ ou que $(1+x)^n$ é a função geradora da seqüência $a_k = \binom{n}{k}$. De maneira análoga, como os coeficientes de x^k na expansão de

$$G(x) = \frac{1}{1-x} = 1 + x + x^2 + x^3 + x^4 + \cdots$$

são todos iguais a 1, diremos que $G(x) = 1/(1-x)$ é a função geradora para a seqüência $a_k = 1$, $k = 0, 1, 2, \ldots$

Como $H(x) = 1/(1-x^2) = 1 + x^2 + x^4 + \cdots$, $H(x)$ é a função geradora para a seqüência $a_k = (1 + (-1)^k)/2$, $k = 0, 1, 2, \ldots$

De um modo geral, a função geradora (ordinária) para a seqüência a_k, $k = 0, 1, 2, \ldots$ é definida como sendo a função $G(x)$ que possui a_k como coeficiente de x^k quando expressa em termos de potências de x, i.e.,

$$G(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + \cdots = \sum_{k=0}^{n} a_kx^k$$

Seguindo esta idéia vamos obter uma função geradora para as partições de n em partes ímpares distintas. Se tomarmos o produto,

$$(1+x)(1+x^3)(1+x^5)(1+x^7)\cdots(1+x^{2k+1})\cdots = 1+x+x^3+x^4+x^5+$$
$$+x^6+x^7+2x^8+2x^9+2x^{10}+2x^{11}+3x^{12}+3x^{14}+3x^{15}+\cdots$$

é fácil ver que o coeficiente de x^6 é igual a 1, que é o total de maneiras de se escrever 6 como soma de ímpares distintos. A potência x^6 aparece como o produto de $x^5 \cdot x^1$. Como 11 só pode ser escrito como soma de ímpares distintos nas formas $11 = 11$ e $11 = 7+3+1$, o coeficiente de x^{11} nesta mesma expressão é igual a 2. O coeficiente de x^{14} é igual a 3. De fato, somente se obtém x^{14} quando se multiplica $x \cdot x^{13}$, $x^3 \cdot x^{11}$ e $x^5 \cdot x^9$. Interpretando-se este produto desta forma, vemos que

$$\prod_{k=0}^{\infty}(1+x^{2k+1}) = \sum_{n=0}^{\infty} d_i(n)x^n,$$

onde $d_i(n)$ é o número de partições de n em partes ímpares distintas, isto é, que

$$\prod_{k=0}^{\infty}(1+x^{2k+1})$$

é a função geradora para $d_i(n)$.

Se estivermos interessados somente nas partições de n em partes distintas devemos tomar o seguinte produto:

$$(1+x)(1+x^2)(1+x^3)(1+x^4)\cdots(1+x^n)\cdots.$$

Como na partição de um número menor do que ou igual a 10 nunca poderemos ter partes superiores a 10, se tomarmos o produto

$$(1+x)(1+x^2)(1+x^3)\cdots(1+x^{10}),$$

teremos a função geradora para as partições de todos os números menores ou iguais a 10 em partes distintas. Como o produto acima é igual a:

$$1+x+x^2+2x^3+2x^4+3x^5+4x^6+5x^7+6x^8+8x^9+10x^{10}+\cdots$$

podemos observar, por exemplo, que, sendo o coeficiente de x^7 igual a 5, existem 5 partições de 7 em partes distintas, que são: 7, $6+1$, $5+2$, $4+3$ e $4+2+1$.

Das observações que acabamos de fazer pode-se concluir que a função geradora para as partições de n em partes distintas é dada pelo produto infinito

$$\prod_{k=1}^{\infty}(1+x^k).$$

Vale mencionar que, como os termos $(1+x^{n+1})$, $(1+x^{n+2})$, ..., não contribuem para as partições de n, para se achar o total de partições de n em partes distintas, basta considerarmos o produto finito $(1+x)(1+x^2)\cdots(1+x^n)$.

Utilizando-se do mesmo argumento anterior é fácil ver que a função geradora para as partições de n em partes pares e distintas é dada por:

$$\prod_{k=1}^{\infty}(1+x^{2k}),$$

e que a função geradora para as partições de n em partes que são quadrados distintos é igual a:

$$\prod_{k=1}^{\infty}(1+x^{k^2}).$$

Como,

$$(1+x)(1+x^4)(1+x^9)(1+x^{16})\cdots =$$
$$= 1+x+x^4+x^5+x^9+x^{10}+x^{13}+x^{14}+x^{16}+\cdots,$$

concluímos que, dentre os números de 1 a 16, somente 8 possuem partições cujas partes são quadrados distintos.

Mostraremos a seguir que a função geradora para $p(n)$, o número de partições de n, é dada por:

$$\sum_{n=0}^{\infty} p(n)x^n = \prod_{k=1}^{\infty}\frac{1}{1-x^k},$$

onde $p(0) = 1$.

Por estarmos mais interessados na interpretação combinatória de $p(n)$ como coeficiente de x^n nesta expansão, vamos demonstrar esta identidade, originalmente apresentada por Euler, utilizando somente argumentos combinatórios. Uma demonstração analítica rigorosa pode ser encontrada em [5] ou [12].

É claro que, sendo

$$\frac{1}{1-x} = 1+x+x^2+x^3+x^4+\cdots;$$

$$\frac{1}{1-x^2} = 1+x^2+x^4+x^6+x^8+\cdots;$$
$$\vdots$$
$$\frac{1}{1-x^m} = 1+x^m+x^{2m}+x^{3m}+\cdots;$$

temos,

$$\prod_{k=1}^{\infty}\frac{1}{1-x^k} = (1+x+x^2+x^3+\cdots)(1+x^2+x^4+x^6+\cdots)$$
$$(1+x^3+x^6+x^9+\cdots)\cdots,$$

donde concluímos que as contribuições para os coeficientes de x^n vêm de um termo x^{a_1} da primeira série, de x^{2a_2} da segunda, de x^{3a_3} da terceira, ..., e de x^{ma_m} da $m^{\text{ésima}}$ série, onde $a_i \geq 0$, para todo i. Sendo o produto destes termos igual a x^n, temos que

$$a_1+2a_2+3a_3+\cdots+ma_m = n.$$

Cada a_i deve ser visto como o número de i's que aparecem na partição de n, isto é, podemos expressar n como

$$n = (1+1+\cdots+1)+(2+2+\cdots+2)+\cdots+(m+m+m+\cdots+m),$$

onde temos a_1 1's no primeiro parênteses, a_2 2's no segundo, a_3 3's no terceiro e a_m m's no $m^{\text{ésimo}}$. Vista desta forma, cada partição de n irá contribuir com uma unidade para o coeficiente de x^n nesta expansão.

Para exemplificar o que acabamos de descrever suponhamos que, em cada uma das primeiras quatro séries, tenhamos tomado, respectivamente, as seguintes potências de x: x^4, x^6, x^6 e x^{12}. Interpretamos estas potências como

$$x^4 = x^{1+1+1+1},$$
$$x^6 = x^{2+2+2},$$
$$x^6 = x^{3+3},$$
$$x^{12} = x^{4+4+4},$$

e, visto que $x^4 \cdot x^6 \cdot x^6 \cdot x^{12} = x^{28}$, temos a seguinte partição de 28:

$$4+4+4+3+3+2+2+2+1+1+1+1.$$

Observe que o x^6 na segunda série representa três 2's e o x^6 na terceira representa dois 3's. Na realidade, as séries acima estão sendo vistas como:

$$\prod_{k=1}^{\infty}\frac{1}{1-x^k} = (1+x^1+x^{1+1}+x^{1+1+1}+\cdots)(1+x^2+x^{2+2}+x^{2+2+2}+\cdots)$$

$$(1+x^3+x^{3+3}+x^{3+3+3}+x^{3+3+3+3}+\cdots)\cdots.$$

A função $1/(1-x)$ "controla", portanto, a presença dos 1's, $1/(1-x^2)$ a presença dos 2's, $1/(1-x^3)$ a presença dos 3's, ..., $1/(1-x^m)$ a presença dos m's. Desta maneira a função geradora para as partições de n em que nenhuma parte supera m é dada por:

$$\prod_{k=1}^{m}\frac{1}{1-x^k}.$$

Listamos na tabela a seguir algumas funções geradoras.

Função Geradora	Para a seqüência das partições de n em partes que são:
$\prod_{k=1}^{\infty}(1+x^{2k+1})$	ímpares distintas
$\prod_{k=1}^{\infty}\frac{1}{(1-x^{2k+1})}$	ímpares
$\prod_{k=1}^{\infty}\frac{1}{(1-x^{2k})}$	pares
$\prod_{k=1}^{\infty}(1+x^{2k})$	pares distintos
$\prod_{k=1}^{\infty}(1+x^{k^3})$	cubos distintos
$\prod_{k=1}^{\infty}\frac{1}{(1-x^{k^3})}$	cubos
$\prod_{p \text{ primo}}\frac{1}{(1-x^p)}$	primos

Voltando à Tabela 9.1, pode-se observar que o número de partições de 5 em partes distintas é igual ao número de partições de 5 em partes ímpares, isto é,

5, 4+1, 3+2, (partes distintas).
5, 3+1+1, 1+1+1+1+1, (partes ímpares).

Com o número 6 ocorre a mesma coisa, isto é, o número de partições em partes distintas é igual ao número de partições em partes ímpares.

6, 5+1, 4+2, 3+2+1, (partes distintas).
5+1, 3+3, 3+1+1+1, 1+1+1+1+1+1, (partes ímpares).

Este fato, na realidade, ocorre para todo n, como provamos no teorema abaixo, devido a Euler.

Teorema 9.5 *O número de partições de n em partes distintas é igual ao número de partições de n em partes ímpares.*

Primeira demonstração: Vamos construir uma correspondência 1–1 entre estes dois tipos de partições. Consideremos uma partição de n em que todas as partes são ímpares. Temos, portanto, a_1 cópias de 1, a_3 cópias de 3, ..., a_{2m+1} cópias de $2m+1$ (onde $2m+1$ é o maior ímpar que ocorre nesta partição). Logo n se escreve como

$$\begin{aligned} n &= 1+\cdots+1+3+\cdots+3+5+\cdots+5+\cdots+ \\ &\quad +(2m+1)+\cdots+(2m+1) \qquad (9.1)\\ &= a_1 1 + a_3 3 + a_5 5+\cdots+a_{2m+1}(2m+1). \end{aligned}$$

Sabemos que cada um dos a_i's pode ser expresso de maneira única como soma de potências distintas de 2 (ver problema resolvido 9.2). Desta forma, temos:

$$\begin{aligned} n &= (2^{\alpha_1}+2^{\alpha_2}+\cdots+2^{\alpha_r})1+(2^{\beta_1}+2^{\beta_2}+\cdots+2^{\beta_s})3 \\ &\quad +\cdots+(2^{y_1}+2^{y_2}+\cdots+2^{y_t})(2m+1) \qquad (9.2)\\ &= 2^{\alpha_1}+2^{\alpha_2}+\cdots+2^{\alpha_r}+3\cdot 2^{\beta_1}+3\cdot 2^{\beta_2}+\cdots+3\cdot 2^{\beta_s}+\cdots \\ &\quad +(2m+1)\cdot 2^{y_1}+(2m+1)\cdot 2^{y_2}+\cdots+(2m+1)\cdot 2^{y_t}. \qquad (9.3) \end{aligned}$$

É claro que todos estes números são distintos entre si, pois os α_i's são todos distintos, assim como os β_i's e os y_i's.

A partição de n em partes ímpares foi transformada em uma partição de n em partes distintas. Para provarmos que este procedimento estabelece a correspondência 1–1 que procuramos, devemos começar, agora, com uma partição de n em que todas as partes são distintas. Cada uma destas diferentes partes pode ser expressa como um produto de um número ímpar vezes uma potência de 2, isto é, n pode ser escrito como uma expressão da forma (9.3). O próximo passo é colocar juntas todas as partes tendo fatores ímpares idênticos. Se colocarmos estes fatores em evidência, teremos uma expressão da forma (9.2). É claro que, somando-se as potências de 2, teremos uma expressão da forma (9.1), que nos fornece a partição de n em partes ímpares, tendo desta forma a correspondência 1–1 que procurávamos. □

Como um exemplo, vamos achar a partição de 96 que está associada, pela correspondência descrita, à seguinte partição em partes ímpares:

$$\begin{aligned} &1+1+1+1+3+5+5+5+7+11+11+15+15+15 = \\ &= 4\cdot 1+1\cdot 3+3\cdot 5+1\cdot 7+2\cdot 11+3\cdot 15 \\ &= 2^2\cdot 1+2^0\cdot 3+(2^1+2^0)\cdot 5+2^0\cdot 7+2^1\cdot 11+(2^1+2^0)\cdot 15 \\ &= 2^2+2^0\cdot 3+2^1\cdot 5+2^0\cdot 5+2^0\cdot 7+2^1\cdot 11+2^1\cdot 15+2^0\cdot 15 \\ &= 4+3+10+5+7+22+30+15 \\ &= 3+4+5+7+10+15+22+30. \end{aligned}$$

Esta última expressão é a partição de 96 em partes distintas.

Segunda demonstração: Utilizamos, agora, funções geradoras. Sabemos que a função geradora para partições em partes distintas é dada por

$$\prod_{k=1}^{\infty}(1+x^k)$$

e que a função geradora para partições em partes ímpares é igual a:

$$\prod_{k=0}^{\infty}\frac{1}{(1-x^{2k+1})}.$$

Basta, portanto, provarmos que estas duas expressões são idênticas. Mas isto segue, uma vez que,

$$\begin{aligned} \prod_{k=1}^{\infty}(1+x^k) &= \prod_{k=1}^{\infty}\frac{(1+x^k)(1-x^k)}{(1-x^k)} \\ &= \prod_{k=1}^{\infty}\frac{(1-x^{2k})}{(1-x^k)} \\ &= \frac{(1-x^2)(1-x^4)(1-x^6)(1-x^8)\cdots}{(1-x)(1-x^2)(1-x^3)(1-x^4)(1-x^5)(1-x^6)\cdots} \\ &= \frac{1}{(1-x)(1-x^3)(1-x^5)(1-x^7)\cdots} \\ &= \prod_{k=1}^{\infty}\frac{1}{(1-x^{2k+1})}. \end{aligned}$$

Como já mencionamos, para os nossos propósitos neste capítulo, a variável x é apenas um símbolo e as questões de convergência não nos preocupam neste momento. □

Apresentamos, a seguir, uma demonstração combinatória para um teorema de Euler conhecido por "O Teorema dos Números Pentagonais de Euler". Este resultado permite a obtenção de uma fórmula de recorrência para o cálculo

de $p(n)$, fórmula esta usada por MacMahon, no princípio do século, para o cálculo de $p(n)$, para $n \leq 200$.

O Teorema de Euler, também conhecido por Fórmula de Euler é o seguinte:

Teorema 9.6 (Fórmula de Euler)

$$\prod_{n=1}^{\infty}(1-x^n) = 1 + \sum_{j=1}^{\infty}(-1)^j(x^{j(3j+1)/2} + x^{j(3j-1)/2}). \qquad (9.4)$$

Pelo fato dos números $1, 5, 12, 22, \ldots, j(3j-1)/2$ serem os números de pontos dentro do j-ésimo pentágono da Figura 9.1 é que este teorema ficou conhecido como Teorema dos Números Pentagonais .

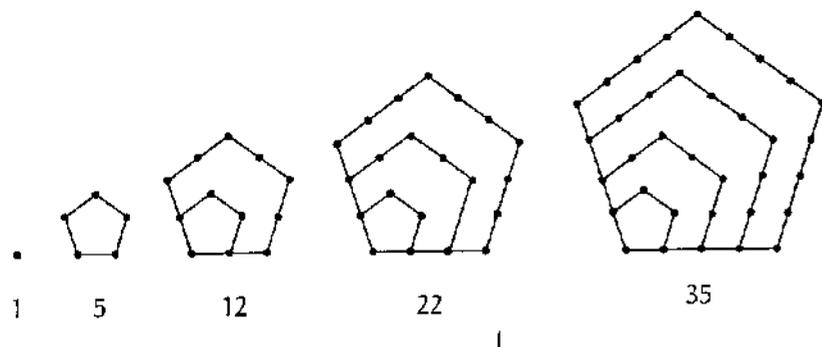



Figura 9.1

Daremos, agora, uma interpretação combinatória para o produto

$$\prod_{n=1}^{\infty}(1-x^n)$$

para que possamos, então, fornecer a demonstração dada por Franklin para (9.4), a qual usa somente argumentos combinatórios.

Legendre observou que (9.4) é equivalente à seguinte igualdade

$$q^e(n) - q^o(n) = \begin{cases} (-1)^j & \text{se } n = j(3j \pm 1)/2 \\ 0 & \text{caso contrário} \end{cases}$$

onde $q^e(n)$ é o número de partições de n em um número par de partes distintas e $q^o(n)$ o número de partições de n em um número ímpar de partes distintas.

Sabemos que

$$\prod_{n=1}^{\infty}(1+x^n)$$

é a função geradora para partições em partes distintas. Isto nos diz, por exemplo, que o coeficiente de x^6 nesta expansão sendo igual a 4 existem exatamente 4 partições de 6 em partes distintas, i.e., $6,\ 5+1,\ 4+2,\ 3+2+1$. Já na expansão de

$$\prod_{n=1}^{\infty}(1-x^n)$$

o coeficiente de x^6 é nulo. É fácil verificar isto pois na expansão de

$$\prod_{n=1}^{\infty}(1-x^n)$$

o produto de um número par de potências distintas de x terá sempre sinal positivo enquanto que o produto de um número ímpar de potências de x terá sempre sinal negativo. Como as partições com um número par de partes distintas resultam do produto de um número par de potências distintas e, analogamente, as partições com um número ímpar de partes distintas resultam do produto de um número ímpar de potências distintas, o coeficiente de x^n será igual a $q^e(n) - q^o(n)$. No exemplo que tomamos, x^6, temos duas partições com um número par de partes distintas $5+1$ e $4+2$ e duas em um número ímpar de partes distintas 6 e $1+2+3$. Por isto o coeficiente de x^6 é zero na expansão de

$$\prod_{n=1}^{\infty}(1-x^n).$$

Com estas considerações fica claro que, como observou Legendre, a fórmula de Euler nos diz que

$$q^e(n) - q^o(n) = \begin{cases} (-1)^j & \text{se } n = j(3j \pm 1)/2 \\ 0 & \text{caso contrário} \end{cases}$$

o que equivale dizer que os números $q^e(n)$ e $q^o(n)$ são iguais exceto quando n é da forma $j(3j \pm 1)/2$ caso em que $q^e(n)$ irá superar $q^o(n)$ por uma unidade, para j par, ou $q^o(n)$ irá superar $q^e(n)$ por uma unidade para j ímpar.

Apresentamos, a seguir, uma demonstração puramente combinatorial para a fórmula de Euler. Esta é, como já mencionamos, a demonstração dada por Franklin em 1881.

A idéia é a de construir uma correspondência $1-1$ entre as partições de n em um número par de partes distintas e as partições de n em um número ímpar de partes distintas.

Utilizamos a representação gráfica para estas partições em que todas as partes são distintas. Nesta representação as partes estão em ordem decrescente. Vamos chamar de a a menor parte desta partição e de b, o número de pontos sobre a linha r mostrada na Figura 9.2.

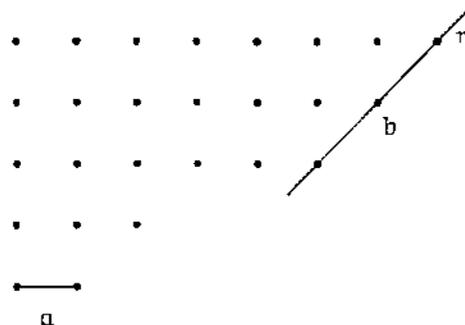



Figura 9.2

Caso $a \leq b$, como na Figura 9.2, podemos remover os "a" pontos da menor parte e colocá-los ao lado dos primeiros "a" pontos da linha r, como mostra a Figura 9.3.

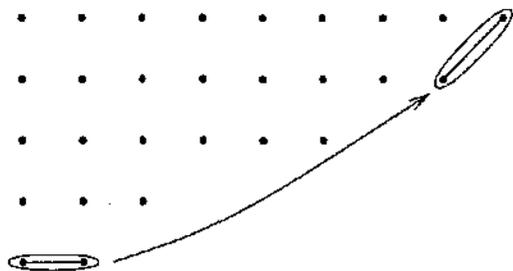



Figura 9.3

Com esta mudança temos agora uma nova partição de n (observe que temos ainda diferentes partes e elas estão dispostas em ordem decrescente) com diferente paridade, isto é, se o total de partes era par, agora é ímpar, e se era ímpar, agora é par. Chamamos a atenção do leitor para o fato de que se o número "a" fosse igual a "b" a mudança acima ainda teria sido possível.

Examinemos, agora, um caso em que $a > b$. Vejamos um exemplo gráfico como aquele mostrado na Figura 9.4. Num caso como este podemos tomar os "b" pontos da linha r e colocá-los abaixo dos "a" pontos obtendo uma nova partição com diferente paridade. Nesta nova partição continuamos com partes

distintas e colocadas em ordem decrescente como podemos ver na Figura 9.5.

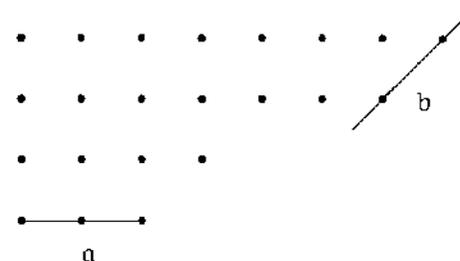



Figura 9.4

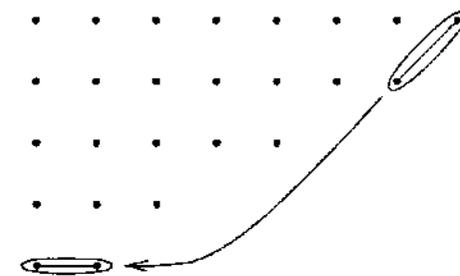



Figura 9.5

É claro que quando uma das duas transformações descritas acima puder ser executada teremos uma correspondência 1-1 entre elementos enumerados por $q^e(n)$ e $q^o(n)$.

Na realidade estas duas transformações não podem ser sempre executadas. Existem exatamente dois casos, ilustrados nas Figuras 9.6 e 9.7, em que a linha r passa através do último ponto da menor parte. Isto ocorre quando $a = b$ ou $a = b + 1$.

É fácil ver que nas duas figuras acima não podemos executar nenhuma das duas transformações descritas. Lembre-se que executada uma destas transformações devemos ter "diferentes partes" e dispostas em "ordem decrescente". Nas Figuras 9.6 e 9.7 temos

$$n = a + (a + 1) + (a + 2) + \cdots + (a + (b - 1)) = \frac{b(2a + b - 1)}{2}.$$

Logo, caso tenhamos uma situação semelhante à da Figura 9.7, isto é,

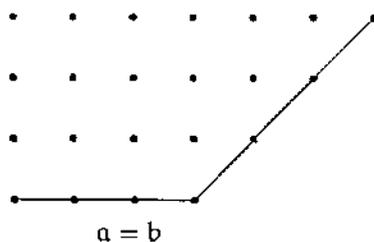



Figura 9.6

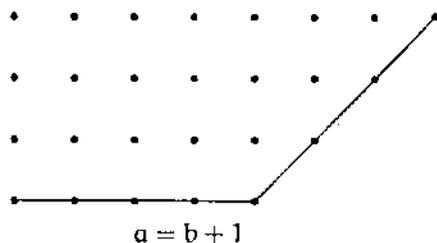



Figura 9.7

$a = b + 1$ teremos,

$$n = \frac{b(3b+1)}{2}.$$

Neste caso se b, o número de partes, for par, teremos $q^e(n) - q^o(n) = 1$ e se b for ímpar, teremos $q^e(n) - q^o(n) = (-1)$. Isto é, teremos exatamente uma partição com um número par (ímpar) de partes excedendo aquelas com um número ímpar (par) de partes.

No caso da Figura 9.6, sendo $a = b$, teremos

$$n = \frac{b(3b-1)}{2}$$

e a mesma análise feita acima será válida, ou seja, $q^e(n) - q^o(n) = (-1)^b$, o que conclui a demonstração. □

Teorema 9.7 *Para todo inteiro positivo* n *temos*

$$\begin{aligned} p(n) &= p(n-1) + p(n-2) - p(n-5) - p(n-7) + \\ &\quad p(n-12) + p(n-15) - p(n-22) - p(n-20) + \cdots \\ &= \sum_j (-1)^{j+1} p\left(n - \frac{j(3j \pm 1)}{2}\right) \end{aligned}$$

onde a soma se extende sobre todos os j *para os quais o argumento da função* $p(n)$ *é não-negativo.*

Demonstração: Já vimos que,

$$\sum_{n=0}^{\infty} p(n)x^n = \prod_{n=1}^{\infty} \frac{1}{1-x^n}$$

e que pela Fórmula de Euler (Teorema 9.4)

$$\prod_{n=1}^{\infty}(1-x^n) = 1 + \sum_{j=1}^{\infty}(-1)^j(x^{j(3j+1)/2} + x^{j(3j-1)/2}).$$

Portanto,

$$\left(1 + \sum_{j=1}^{\infty}(-1)^j(x^{j(3j+1)/2} + x^{j(3j-1)/2})\right)\sum_{n=0}^{\infty} p(n)x^n = 1$$

isto é,

$$\begin{aligned} &(1 - x - x^2 + x^5 + x^7 - x^{12} - x^{15} + x^{22} + x^{26} + \cdots)\sum_{n=0}^{\infty} p(n)x^n = \\ &\sum_{n=0}^{\infty} p(n)x^n - \sum_{n=0}^{\infty} p(n)x^{n+1} - \sum_{n=0}^{\infty} p(n)x^{n+2} + \sum_{n=0}^{\infty} p(n)x^{n+5} + \cdots \\ &= \sum_{n=0}^{\infty} p(n)x^n - \sum_{n=1}^{\infty} p(n-1)x^n - \sum_{n=2}^{\infty} p(n-2)x^n + \sum_{n=5}^{\infty} p(n-5)x^n + \cdots = 1 \end{aligned}$$

Igualando-se o coeficiente de x^n em ambos os lados da identidade acima temos,

$$\begin{aligned} &p(n) - p(n-1) - p(n-2) + p(n-5) + p(n-7) \\ &-p(n-12) - p(n-15) + p(n-22) + p(n-26) - \cdots = 0 \end{aligned}$$

e isto conclui a demonstração. □

9.4 Problemas Resolvidos

Problema 9.1 Provar que, para $1 \leq j \leq n$, o número de partições de n nas quais j aparece como parte é igual ao número de partições de $n - j$.

Solução. Precisamos exibir uma aplicação 1–1 entre estas duas famílias descritas. É claro que, se a cada partição de $n - j$ acrescentarmos uma nova parte igual a j, teremos uma partição de n tendo j como parte. Obviamente, se em

uma partição de n, contendo j como parte, retirarmos j (uma parte igual a j), teremos uma partição de $n-j$, o que completa a demonstração.

Problema 9.2 Provar que todo inteiro positivo pode ser expresso de maneira única como soma de potências distintas de 2.

Solução. Pelos argumentos apresentados neste capítulo, é fácil ver que a função

$$(1+x)(1+x^2)(1+x^4)(1+x^8)\cdots(1+x^{2^k})\cdots \tag{9.5}$$

é a função geradora para as partições de n em partes que são potências distintas de 2. Logo, o coeficiente de x^n nesta expansão nos fornece o número de maneiras de se escrever n como soma de potências distintas de 2. Portanto, para provarmos o que foi pedido, basta mostrarmos que o coeficiente de x^n em (9.5) é igual a 1, para todo n. Mas sendo

$$\frac{1}{1-x} = 1+x+x^2+x^3+x^4+\cdots,$$

será suficiente provarmos a igualdade seguinte:

$$\frac{1}{1-x} = (1+x)(1+x^2)(1+x^4)(1+x^8)\cdots(1+x^{2^k})\cdots.$$

Mas isto ocorre, uma vez que

$$\begin{aligned}(1-x)(1+x)(1+x^2)(1+x^4)(1+x^8)\cdots &= \\ &= (1-x^2)(1+x^2)(1+x^4)(1+x^8)(1+x^{16})\cdots \\ &= (1-x^4)(1+x^4)(1+x^8)(1+x^{16})(1+x^{32})\cdots \\ &= (1-x^8)(1+x^8)(1+x^{16})(1+x^{32})(1+x^{64})\cdots \\ &= (1-x^{16})(1+x^{16})(1+x^{32})(1+x^{64})\cdots \\ &= 1,\end{aligned}$$

o que conclui a demonstração.

Problema 9.3 Provar que o número de partições de n em exatamente 2 partes é igual a $\lfloor \frac{n}{2} \rfloor$, isto é, que $q_2(n) = \lfloor \frac{n}{2} \rfloor$.

Solução. Vamos calcular, primeiro, o número de partições de n em no máximo duas partes. Sabemos, pelo Corolário 9.2, que este número é igual ao número de partições de n em que nenhuma parte supera 2. Como a função geradora para partições em que as partes são menores do que ou iguais a 2 é dada por:

$$\frac{1}{(1-x)(1-x^2)},$$

devemos calcular o coeficiente de x^n nesta expansão, o qual nos dará o número de partições de n com partes menores do que ou iguais a 2. Mas como

$$\frac{1}{(1-x)(1-x^2)} = \frac{1}{2(1-x)^2} + \frac{1}{2(1-x^2)}, \tag{9.6}$$

devemos achar o coeficiente de x^n em cada uma das expressões do lado direito de (9.6). Como

$$\frac{1}{2(1-x)^2} = \frac{1}{2}(1+x+x^2+x^3+\cdots)(1+x+x^2+x^3+\cdots),$$

o coeficiente de x^n nesta expressão é igual a $(n+1)/2$, e o coeficiente de x^n em

$$\frac{1}{2(1-x^2)} = \frac{1}{2}(1+x^2+x^4+x^6+\cdots)$$

é igual a $1/2$, se n for par, e zero, caso contrário. Logo, o coeficiente de x^n em $1/(1-x)(1-x^2)$ é igual à soma destes dois coeficientes, sendo, portanto, dado por:

$$\frac{n+1}{2}, \quad \text{se } n \text{ for ímpar,}$$

e

$$\frac{n+1}{2} + \frac{1}{2} = \frac{n+2}{2}, \quad \text{se } n \text{ for par.}$$

Mas se n for par, isto é, $n = 2k$,

$$\frac{n+2}{2} = \frac{2k+2}{2} = k+1 = \left\lfloor \frac{n}{2} \right\rfloor + 1$$

e, se n for ímpar, isto é, $n = 2k+1$,

$$\frac{n+1}{2} = \frac{2k+1+1}{2} = \frac{2k+2}{2} = k+1 = \left\lfloor \frac{n}{2} \right\rfloor + 1.$$

Com isto provamos que o número de partições de n em partes menores do que ou iguais a 2, que é igual ao número de partições em no máximo duas partes, é igual a:

$$\left\lfloor \frac{n}{2} \right\rfloor + 1.$$

Como só existe uma partição de n tendo exatamente uma parte, concluímos que o número pedido é igual a $\lfloor \frac{n}{2} \rfloor$.

Problema 9.4 Mostrar que o número de partições de n em partes distintas, nenhuma sendo múltipla de 3, é igual ao número de partições de n em partes da forma $6j-1$ ou $6j-5$.

Solução. É fácil ver que a função geradora para partições de n em partes distintas e não-divisíveis por 3 é dada por

$$\prod_{j=1}^{\infty}(1+x^{3j-2})(1+x^{3j-1}), \tag{9.7}$$

e que a função geradora para as partições de n em partes da forma $6j-1$ ou $6j-5$ é igual a

$$\prod_{j=1}^{\infty}\frac{1}{(1-x^{6j-1})(1-x^{6j-5})}. \tag{9.8}$$

Portanto, devemos mostrar a igualdade entre (9.7) e (9.8). Mas isto segue, pois

$$\begin{aligned}\prod_{j=1}^{\infty}(1+x^{3j-2})(1+x^{3j-1}) &= \prod_{j=1}^{\infty}\frac{(1+x^{3j-2})(1+x^{3j-1})(1-x^{3j-2})(1-x^{3j-1})}{(1-x^{3j-2})(1-x^{3j-1})}\\ &= \prod_{j=1}^{\infty}\frac{(1-x^{6j-4})(1-x^{6j-2})}{(1-x^{3j-2})(1-x^{3j-1})}\\ &= \prod_{j=1}^{\infty}(1-x^{6j-4})(1-x^{6j-2})\prod_{j=1}^{\infty}\frac{1}{(1-x^{3j-2})(1-x^{3j-1})}\\ &= \prod_{j=1}^{\infty}(1-x^{6j-4})(1-x^{6j-2})\prod_{j=1}^{\infty}\frac{1}{(1-x^{6j-4})(1-x^{6j-1})(1-x^{6j-5})(1-x^{6j-2})}\\ &= \prod_{j=1}^{\infty}\frac{1}{(1-x^{6j-1})(1-x^{6j-5})},\end{aligned}$$

o que conclui a demonstração.

Problema 9.5 Encontrar a função geradora para o número de triângulos não-semelhantes de perímetro n e lados inteiros.

Solução. Sejam a, b e c as medidas dos lados de um triângulo. Como estamos interessados em triângulos não-semelhantes podemos considerar

$$a \le b \le c. \tag{9.9}$$

Para evitar lados nulos tomamos

$$a \ge 1, \tag{9.10}$$

e, para que exista um triângulo de lados a, b e c, devemos ter

$$a+b>c. \tag{9.11}$$

É fácil observar que

$$a+b+c = 3a+2(b-a)+c-b = 3a+2y+z = n, \tag{9.12}$$

onde $y = b-a$ e $z = c-b$.

Agora, (9.9) é equivalente a

$$y \ge 0 \quad \text{e} \quad z \ge 0,$$

e (9.11) pode ser reescrita como

$$a > z. \tag{9.13}$$

Sendo a, b, c, y e z inteiros, (9.13) e (9.10) podem ser substituídas por

$$\begin{aligned} a &= z+x,\\ x &\ge 1.\end{aligned}$$

Substituindo estes valores em (9.12) obtemos

$$\begin{aligned}&3x+2y+4z = n,\\ &x\ge 1,\ y\ge 0,\ z\ge 0.\end{aligned}$$

Esta última equação nos permite escrever, facilmente, a função geradora procurada:

$$\begin{aligned}&(x^3+x^6+x^9+\cdots)(1+x^2+x^4+\cdots)(1+x^4+x^8+\cdots) =\\ &= \frac{x^3}{1-x^3}\cdot\frac{1}{1-x^2}\cdot\frac{1}{1-x^4} = \frac{x^3}{(1-x^2)(1-x^3)(1-x^4)}.\end{aligned} \tag{9.14}$$

Problema 9.6 Obter uma fórmula explícita para a contagem do número de triângulos não-semelhantes de lados inteiros e perímetro n.

Solução. No Corolário 9.2 vimos que o número de partições de n em no máximo k partes é igual ao número de partições de n em que nenhuma parte supera k.

Logo, para encontrarmos o número de partições de n, em no máximo 3 partes, precisamos encontrar o coeficiente de x^n em

$$\frac{1}{(1-x)(1-x^2)(1-x^3)}, \tag{9.15}$$

que é a função geradora para partições em que nenhuma parte supera 3. Como

$$\frac{1}{(1-x)(1-x^2)(1-x^3)} = \frac{1}{6(1-x)^3} + \frac{1}{4(1-x)^2} + \frac{1}{4(1-x^2)} + \frac{1}{3(1-x^3)}$$

e

$$\frac{1}{6(1-x)^3} = \frac{1}{6}(1-x)^{-3} = \frac{1}{6}\sum_{n=0}^{\infty}\binom{-3}{n}(-1)^n x^n$$

$$= \sum_{n=0}^{\infty}\frac{1}{6}\frac{(n+2)(n+1)}{2}x^n, \tag{9.16}$$

$$\frac{1}{4}\frac{1}{(1-x)^2} = \frac{1}{4}(1-x)^{-2} = \frac{1}{4}\sum_{n=0}^{\infty}\binom{-2}{n}(-1)^n x^n$$

$$= \sum_{n=0}^{\infty}\frac{(n+1)}{4}x^n, \tag{9.17}$$

$$\frac{1}{4(1-x^2)} = \frac{1}{4}(1+x^2+x^4+x^6+\cdots), \tag{9.18}$$

$$\frac{1}{3(1-x^3)} = \frac{1}{3}(1+x^3+x^6+x^9+\cdots), \tag{9.19}$$

concluímos que o coeficiente de x^n em (9.15) é igual a:

$$\begin{array}{lll} \frac{1}{12} & (n^2+6n+5+7), & \text{para } n \text{ par e divisível por } 3; \\ \frac{1}{12} & (n^2+6n+5+3), & \text{para } n \text{ par e não-divisível por } 3; \\ \frac{1}{12} & (n^2+6n+5+4), & \text{para } n \text{ ímpar e divisível por } 3; \\ \frac{1}{12} & (n^2+6n+5), & \text{para } n \text{ ímpar e não-divisível por } 3. \end{array} \tag{9.20}$$

Pode-se observar que a diferença entre cada um destes quatro números acima (todos são inteiros) e o número $\frac{(n+3)^2}{12}$ é menor do que $1/2$ e, portanto, o coeficiente de x^n em (9.15) é o inteiro mais próximo de $\frac{(n+3)^2}{12}$ que denotamos por $\left\{\frac{(n+3)^2}{12}\right\}$. Logo $\left\{\frac{(n+3)^2}{12}\right\}$ é o número de partições de n em no máximo 3 partes.

A demonstração que apresentamos abaixo segue Andrews [4]. Ele observou que cada partição de n em exatamente 3 partes nos fornece um único triângulo do tipo que queremos e reciprocamente, exceto quando a soma das duas menores partes não superam a maior parte. Sendo a, b e c as três partes, $1 \le a \le b \le c$, isto irá ocorrer para cada partição de j em duas partes a e b com $1 \le j \le \frac{n}{2}$, pois neste caso $a+b+(n-j)$ será uma partição de n em 3 partes com $a+b \le n-j$ e isto não nos permite a construção de nenhum triângulo.

Devemos, pois, subtrair do número total de partições de n em exatamente 3 partes o número de partições de j em duas partes, para $j = 1, 2, 3, \ldots, [n/2]$. Logo devemos calcular a soma $q_2(2) + q_2(3) + \ldots + q_2(\lfloor n/2 \rfloor)$ e subtrair do número total de partições de n em exatamente 3 partes. Lembre-se que $q_2(j)$ denota o número de partições de j em exatamente 2 partes.

Vimos, acima, que o número de partições de n em no máximo 3 partes é $\left\{\frac{(n+3)^2}{12}\right\}$. Sabemos, pelo Exemplo 9.3, que o número de partições de n em no máximo 2 partes é $\lfloor \frac{n}{2} \rfloor + 1$. Logo a diferença

$$\left\{\frac{(n+3)^2}{12}\right\} - \left(\left\lfloor\frac{n}{2}\right\rfloor + 1\right)$$

nos fornece o número total de partições de n em exatamente 3 partes.

Pode-se ver, basta considerar os casos n par e n ímpar e as equações (9.20), que a diferença acima é igual a

$$\left\{\frac{n^2}{12}\right\}. \tag{9.21}$$

Precisamos, pois, subtrair deste número a soma $q_2(2)+q_2(3)+\cdots+q_2(\lfloor n/2 \rfloor)$.

Provamos, por indução, que esta soma é igual a $\left\lfloor\frac{n}{4}\right\rfloor\left\lfloor\frac{n+2}{4}\right\rfloor$, isto é,

$$\left\lfloor\frac{2}{2}\right\rfloor + \left\lfloor\frac{3}{2}\right\rfloor + \cdots + \left\lfloor\frac{\lfloor n/2 \rfloor}{2}\right\rfloor = \left\lfloor\frac{n}{4}\right\rfloor\left\lfloor\frac{n+2}{4}\right\rfloor \tag{9.22}$$

uma vez que $q_2(j) = \lfloor j/2 \rfloor$ como foi mostrado no Problema 9.3.

Para n par é fácil observar que

$$\left\lfloor\frac{n}{2}\right\rfloor = \left\lfloor\frac{n+1}{2}\right\rfloor, \left\lfloor\frac{n}{4}\right\rfloor = \left\lfloor\frac{n+1}{4}\right\rfloor \text{ e } \left\lfloor\frac{n+2}{4}\right\rfloor = \left\lfloor\frac{n+3}{4}\right\rfloor$$

e, portanto, a demonstração por indução segue imediatamente.

Para n ímpar consideramos os casos $n \equiv 1 (\mathrm{mod}\ 4)$ e $n \equiv 3 (\mathrm{mod}\ 4)$. Se $n \equiv 1 (\mathrm{mod}\ 4)$ temos

$$\left\lfloor \frac{2}{2} \right\rfloor + \left\lfloor \frac{3}{2} \right\rfloor + \cdots + \left\lfloor \frac{\lfloor n/2 \rfloor}{2} \right\rfloor + \left\lfloor \frac{\lfloor (n+1)/2 \rfloor}{2} \right\rfloor = \left\lfloor \frac{n}{4} \right\rfloor \left\lfloor \frac{n+2}{4} \right\rfloor + \left\lfloor \frac{\lfloor (n+1)/2 \rfloor}{2} \right\rfloor$$
$$= \left\lfloor \frac{n}{4} \right\rfloor \left\lfloor \frac{n+2}{4} \right\rfloor + \left\lfloor \frac{n}{4} \right\rfloor = \left\lfloor \frac{n}{4} \right\rfloor \left(\left\lfloor \frac{n+2}{4} \right\rfloor + 1 \right) = \left\lfloor \frac{n+1}{4} \right\rfloor \left\lfloor \frac{n+3}{4} \right\rfloor,$$

uma vez que para $n \equiv 1 (\mathrm{mod}\ 4)$

$$\left\lfloor \frac{\lfloor (n+1)/2 \rfloor}{2} \right\rfloor = \left\lfloor \frac{n+1}{4} \right\rfloor = \left\lfloor \frac{n}{4} \right\rfloor \text{ e } \left\lfloor \frac{n+2}{4} \right\rfloor + 1 = \left\lfloor \frac{n+3}{4} \right\rfloor.$$

Para $n \equiv 3 (\mathrm{mod}\ 4)$ temos

$$\left\lfloor \frac{2}{2} \right\rfloor + \left\lfloor \frac{3}{2} \right\rfloor + \cdots + \left\lfloor \frac{\lfloor n/2 \rfloor}{2} \right\rfloor + \left\lfloor \frac{\lfloor (n+1)/2 \rfloor}{2} \right\rfloor = \left\lfloor \frac{n}{4} \right\rfloor \left\lfloor \frac{n+2}{4} \right\rfloor + \left\lfloor \frac{\lfloor n/2 \rfloor}{2} \right\rfloor + 1$$
$$= \left\lfloor \frac{n}{4} \right\rfloor \left\lfloor \frac{n+2}{4} \right\rfloor + \left\lfloor \frac{n+3}{4} \right\rfloor = \left\lfloor \frac{n}{4} \right\rfloor \left\lfloor \frac{n+3}{4} \right\rfloor + \left\lfloor \frac{n+3}{4} \right\rfloor$$
$$= \left(\left\lfloor \frac{n}{4} \right\rfloor + 1 \right) \left\lfloor \frac{n+3}{4} \right\rfloor = \left\lfloor \frac{n+1}{4} \right\rfloor \left\lfloor \frac{n+3}{4} \right\rfloor,$$

uma vez que

$$\left\lfloor \frac{\lfloor (n+1)/2 \rfloor}{2} \right\rfloor = \left\lfloor \frac{\lfloor n/2 \rfloor}{2} \right\rfloor + 1 = \left\lfloor \frac{n+3}{4} \right\rfloor,$$
$$\left\lfloor \frac{n+2}{4} \right\rfloor = \left\lfloor \frac{n+3}{4} \right\rfloor \text{ e } \left\lfloor \frac{n}{4} \right\rfloor + 1 = \left\lfloor \frac{n+1}{4} \right\rfloor.$$

Subtraindo do número total de partições de n em exatamente 3 partes, dado em (9.21), o número de partições de n em 3 partes que não nos permite a construção de triângulos, dado em (9.22), obtemos, finalmente, que o total *de triângulos não-semelhantes de perímetro n e lados inteiros* é igual a

$$\left\{ \frac{n^2}{12} \right\} - \left\lfloor \frac{n}{4} \right\rfloor \left\lfloor \frac{n+2}{4} \right\rfloor.$$

9.5 Problemas Propostos

1. Encontrar a função geradora ordinária para cada uma das seqüências abaixo:

(a) $(1, 1, 1, 0, 0, 0, \ldots)$; (b) $(1, 0, 0, 2, 3, 0, 0, 0, \ldots)$;

(c) $(1, 1, 1, 3, 1, 1, \ldots)$; (d) $(0, 0, 1, 1, 1, \ldots)$;

(e) $(0, 1, 0, 1, 0, 1, \ldots)$; (f) $(0, 4, 0, 4, 0, 4, \ldots)$;

(g) $(1, -1, 1, -1, 1, -1, \ldots)$; (h) $\left(1, -1, \frac{1}{2!}, \frac{-1}{3!}, \frac{1}{4!}, \frac{-1}{5!}, \ldots\right)$;

(i) $(a_k) = \left(\frac{2^k}{k!}\right)$.

2. Encontrar a seqüência gerada por cada função geradora ordinária dada abaixo:

(a) $(x+1)^4$; (b) $x + e^x$;

(c) $x^2(1-3x)^{-1}$; (d) $1 + (1-x^2)^{-1}$;

(e) $e^{2x} + x + x^2$; (f) $x^2 e^x$;

3. Quantas soluções possui a equação $x_1 + x_2 + x_3 + \cdots + x_n = r$, se cada variável é igual a 0 ou 1?

4. Encontrar as funções geradoras ordinárias que permitem o cálculo do número de maneiras de se distribuir 11 laranjas e 6 peras para 3 crianças de modo que cada criança receba pelo menos 3 laranjas e no máximo 2 peras.

5. Encontrar a função geradora ordinária que permita a obtenção de resposta à seguinte pergunta: de quantas maneiras podemos distribuir 300 cadeiras idênticas em 4 salas de modo que o número de cadeiras em cada sala seja 20 ou 40 ou 60 ou 80 ou 100?

6. Encontrar a função geradora ordinária para o número de partições de n em que todas as partes são ímpares e nenhuma supera 7.

7. Dar uma interpretação, em termos de partições, para:

(a) O coeficiente de x^{12} na expansão de

$$(1 + x^2 + x^4 + x^6 + x^8 + x^{10} + x^{12})(1 + x^4 + x^8 + x^{12})$$
$$(1 + x^6 + x^{12})(1 + x^8)(1 + x^{10})(1 + x^{12}).$$

(b) O coeficiente de x^{15} na expansão de

$$(1 + x^3 + x^6 + x^9 + x^{12} + x^{15})(1 + x^6 + x^{12})(1 + x^9).$$

8. Calcular os coeficientes dos itens (a) e (b) do exercício anterior.

9. Escrever a função geradora que pode ser usada para se encontrar:

(a) O número de partições de 34 com partes restritas a 6, 8, 10 e 20.

(b) O número de partições de 13 com partes maiores do que 3.

(c) O número de partições de 11 em partes ímpares distintas.

10. Mostrar que para todo m par ≥ 6 o número de partições de n em partes ímpares é maior que o número de partições de n em partes pares.

Apêndice A

Os Princípios da Boa Ordem e da Indução Finita.

Estes princípios, já enunciados no primeiro capítulo, são os seguintes:

A_0: **Princípio da Boa Ordem (PBO)** *Todo conjunto não-vazio de inteiros positivos contém um elemento mínimo.*

A_1: **Primeira forma do Princípio de Indução Finita** *Seja* B *um subconjunto dos inteiros positivos. Se* B *possui as duas seguintes propriedades*

(i) $1 \in B$

(ii) $k+1 \in B$ *sempre que* $k \in B$

então B *contém todos os inteiros positivos.*

A_2: **Segunda forma do Princípio de Indução Finita** *Seja* B *um subconjunto dos inteiros positivos. Se* B *possui as duas seguintes propriedades*

(i) $1 \in B$

(ii) $k+1 \in B$ *sempre que* $1, 2, \ldots, k \in B$

então B *contém todos os inteiros positivos.*

Devemos mostrar que $A_0 \Rightarrow A_1, A_1 \Rightarrow A_2$ e $A_2 \Rightarrow A_0$. Como no capítulo 1 já mostramos a implicação $A_0 \Rightarrow A_1$, mostraremos aqui apenas as outras duas.

Teorema A.1. $A_1 \Rightarrow A_2$

esta série diverge. Para ver isto basta lembrar a divergência da série harmônica e considerar que

$$\frac{1}{1+nQ} > \frac{1}{Q+nQ} = \frac{1}{Q}\frac{1}{(1+n)},$$

o que conclui a demonstração.

A segunda prova que apresentamos, dada por P. Schorn , segue a idéia de que, para mostrarmos que existem infinitos primos, é suficiente exibir uma seqüência infinita de inteiros positivos que sejam relativamente primos.

Observamos que se $1 \leq i < j \leq n$ então $((n!)i+1, (n!)j+1) = 1$.

Na realidade escrevendo $j = i + d$, então $1 \leq d < n$ e

$$((n!)i+1, (n!)j+1) = ((n!)i+1, (n!)d) = 1$$

pois todo primo dividindo $(n!)d$ é no máximo igual a n.

Logo, se o número de primos fosse igual a m, tomando $n = m+1$, a observação acima implica que os $m+1$ inteiros $(m+1)!\,i+1$ $(1 \leq i \leq m+1)$ seriam primos entre si, i.e., existiriam pelo menos $m+1$ primos distintos, o que contraria nossa hipótese.

Apêndice C

O Postulado de Bertrand

Na demonstração do Postulado de Bertrand faremos uso de três resultados elementares que apresentamos no Lema abaixo.

Lema C. *Para* $n \geq 1$ *temos*

(i) Seja $r(p)$ satisfazendo $p^{r(p)} \leq 2n < p^{r(p)+1}$, então

$$\binom{2n}{n} \Big| \prod_{p \leq 2n} p^{r(p)}.$$

(ii) Se $n > 2$ e $2n/3 < p \leq n$, então $p \nmid \binom{2n}{n}$.

(iii) $\prod_{p \leq n} p < 4^n$.

Demonstração: (i) O expoente de p em $n!$ sendo igual a $\sum_{j=1}^{r(p)} \lfloor n/p^j \rfloor$ (ver Teorema 4.9) nos diz que o expoente de p em $\binom{2n}{n}$ é dado por

$$\sum_{j=1}^{r(p)} (\lfloor 2n/p^j \rfloor - 2\lfloor n/p^j \rfloor) \leq \sum_{j=1}^{r(p)} 1 = r(p).$$

Esta última desigualdade se verifica pois, pelo teorema 4.8(7), $\lfloor 2x \rfloor - 2\lfloor x \rfloor$ é igual a 0 ou 1. Para concluir a demonstração basta tomar o produto sobre os primos $p \leq 2n$.

(ii) Se p satisfaz $2n/3 < p \leq n$ então p ocorre uma vez na fatoração de $n!$ e duas vezes na fatoração de $(2n)!$, pois $3p > 2n$. Logo, como $p > 2, p \nmid \binom{2n}{n}$

(iii) Isto será provado por indução.

Seja $P(n)$ a proposição a ser provada. É fácil ver que $P(n)$ é verdadeira para $n = 1, 2$ e 3. Para $m > 1$ temos que $P(2m-1)$ implica $P(2m)$ pois

$$\prod_{p \leq 2m} p = \prod_{p \leq 2m-1} p < 4^{2m-1} < 4^{2m}.$$

Desta forma, podemos supor $n = 2m+1$ com $m \geq 2$. Como todo primo p no intervalo $[m+2, 2m+1]$ é um fator de $\binom{2m+1}{m}$, teremos (assumindo que $P(m+1)$ se verifica):

$$\prod_{p \leq 2m+1} p \leq \binom{2m+1}{m} \prod_{p \leq m+1} p < \binom{2m+1}{m} 4^{m+1}. \tag{C.1}$$

Mas

$$\binom{2m+1}{m} < \frac{1}{2}(1+1)^{2m+1} = 4^m$$

pois $\binom{2m+1}{m}$ corresponde aos dois termos centrais da expansão binomial de $(1+1)^{2m+1}$.

Logo, por (C.1) vemos que $P(m+1)$ implica $P(2m+1)$, o que completa a prova por indução.

O Postulado de Bertrand *Para cada inteiro positivo* n *existe um primo* p *satisfazendo* $n < p \leq 2n$.

Demonstração: Claramente o resultado é verdadeiro para $n \leq 3$. Nós vamos assumir que o resultado seja falso para algum $n > 3$ e obter uma contradição. Temos do Lema C(ii) que para este n todos os fatores primos p de $\binom{2n}{n}$ satisfazem $p \leq 2n/3$. Seja $s(p)$ a maior potência de p a qual divide $\binom{2n}{n}$. Logo pelo Lema C.1.(i) temos que

$$p^{s(p)} \leq 2n. \tag{C.2}$$

Portanto se $s(p) > 1$ então $p \leq \sqrt{2n}$ e segue que no máximo $\lfloor \sqrt{2n} \rfloor$ primos ocorrem em $\binom{2n}{n}$ com expoente maior do que 1.

Usando (C.2) e nossa suposição obtemos

$$\binom{2n}{n} \leq (2n)^{\lfloor \sqrt{2n} \rfloor} \prod_{p \leq 2n/3} p.$$

Mas $\frac{4^n}{2n+1} < \binom{2n}{n}$, uma vez que $\binom{2n}{n}$ é o maior termo na expansão binomial de $(1+1)^{2n}$, a qual possui $2n+1$ termos.

Desta forma, usando o Lema C.1.(iii) e estas duas desigualdades obtemos

$$\frac{4^n}{2n+1} < (2n)^{\lfloor \sqrt{2n} \rfloor} \prod_{p \leq 2n/3} p < 4^{2n/3}(2n)^{\sqrt{2n}}.$$

Sendo $2n+1 < (2n)^2$, podemos cancelar $4^{2n/3}$ do 1º e 3º membros da expressão acima para obtermos

$$4^{n/3} < (2n)^{2+\sqrt{2n}}.$$

Disto temos

$$\frac{n \ln 4}{3} < (2 + \sqrt{2n}) \ln 2n.$$

Claramente isto é falso para n grande. De fato se $n = 750$ temos $(1.3 < \ln 4$ e $\ln 1500 < 7.5)$

$$325 = \frac{750 \times 1.3}{3} < (2 + \sqrt{1500}) \ln(1500) < 41 \times 7.5 < 308.$$

Portanto o resultado é verdadeiro para $n \geq 750$ e, por inspeção, ele também se verifica para $n < 750$, como pode ser visto pela seqüência 2, 3, 5, 7, 13, 23, 43, 83, 163, 317, 631, 751 de primos na qual cada um é menor do que duas vezes o seu predecessor.

Bibliografia

[1] ALENCAR FILHO, Edgard de. **Teoria elementar dos números**. São Paulo: Nobel, 1992. 336 p.

[2] ANDREWS, George E. **The theory of partitions**. Cambridge: Cambridge University Press, 1984. 255 p.

[3] ANDREWS, George E. **Number theory**. New York: Dover, 1994. 259 p.

[4] ANDREWS, George E. A note on partitions and triangles with integer sides. **American Math. Monthly 86**, 1979, p. 477-478.

[5] APOSTOL, Tom M. **Introduction to analytic number theory**. New York: Springer-Verlag, 1976. 338 p.

[6] CLARKSON, J. A. On the series of prime reciprocals. **Proceedings of the American Mathematical Society**, v. 17, n. 2, p. 541, April 1966.

[7] DAVENPORT, Harold. **The higher arithmetic**: an introduction to the theory of numbers. New York: Dover, 1983. 172 p.

[8] DOMINGUES, H. H. **Fundamentos de aritmética**. São Paulo: Atual, 1991. 297 p.

[9] ERDÖS, P., SZEKERES, G. A combinatorial problem in geometry. **Compositio mathematica**, Croningen, v. 2, p. 464-470, 1935.

[10] FIGUEIREDO, D. G. **Números irracionais e transcendentes**. Rio de Janeiro: Sociedade Brasileira de Matemática, 1985. 101 p. (Coleção Fundamentos da Matemática Elementar).

[11] GROSSWALD, Emil. **Representations of integers as sums of square**. New York: Springer-Verlag, 1985. 251 p.

[12] HARDY, G. H., WRIGHT, Edward M. **An introduction to the theory of numbers**. 4. ed. Oxford: Clarendon Press, 1962. 421 p.

[13] HSIUNG, C. Y. **Elementary theory of numbers**. Singapore, New Jersey: World Scientific, 1992. 250 p.

[14] INGHAM, A. E. **The distribution of prime numbers**. Cambridge, New York: Cambridge University Press, 1990. 114 p.

[15] IRELAND, K., ROSEN, M. **A classical introduction to modern number theory**. New York: Springer-Verlag, 1990. 341 p.

[16] LEQUAIN, Y. **Aproximação de um número real por números racionais**. Rio de Janeiro: IMPA, 1993. 152 p.

[17] LEVEQUE, W. J. **Elementary theory of number**. New York: Dover, 1990. 132 p.

[18] LONG, C. T. **Elementary introduction to number theory**. 2. ed. Lexington, Mass: D. C. Heath, 1972. 239 p.

[19] NAGELL, Trygve. **Introduction to number theory**. New York: Chelsea, 1964. 309 p.

[20] NIVEN, Ivan Morton. **Mathematics of choice**: how to count without counting. Washington: Mathematical Association of America, 1965. 216 p.

[21] NIVEN, Ivan M., ZUCKERMAN, Herbert S., MONTGOMERY, Hugh L. **An introduction to the theory of numbers**. New York: John Wiley & Sons, 1991. 529 p.

[22] OLDS, C. D. **Continued fractions**. Washington: Mathematical Association of America, 1963. 162 p.

[23] ORE, Oystein. **Number theory and its history**. New York: Dover, 1988. 370 p.

[24] PARENT, D. P. **Exercises in number theory**. New York: Springer-Verlag, 1984. 541 p.

[25] POLLARD, Harry, DIAMOND, Harold G. **The theory of algebraic numbers**. 2. ed. Washington: Mathematical Association of America, 1975. 162 p.

[26] RIBENBOIM, Paulo. **The little book of big primes**. New York: Springer-Verlag, 1991. 237 p.

[27] ROSE, H. E. **A course in number theory**. Oxford, New York: Clarendon Press, Oxford University Press, 1995. 398 p.

[28] ROSEN, Kenneth H. **Elementary number theory and its applications**. Reading, Mass: Addison-Wesley, 1984. 452 p.

[29] SANTOS, José Plínio de O., MELLO, Margarida P., MURARI, Idani T. C. **Introdução à análise combinatória**. Campinas: Editora da UNICAMP, 1995. 295 p.

[30] SIERPINSKI, Waclaw. **250 problems in elementary number theory**. New York: American Elsevier Publishing Company, 1970. 125 p.

[31] SHOKRANIAN, S., SOARES, M., GODINHO, H. **Teoria dos números.** Brasília: Editora da Universidade de Brasília, 1994. 336 p.

[32] SIDKI, Said. **Introdução à teoria dos números.** Rio de Janeiro: IMPA, 1975. 186 p.

Índice